UNIVERSIDAD DE PAMPLONA
FACULTAD DE INGENIERÍAS Y ARQUITECTURA
DEPARTAMENTO DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, SISTEMAS Y TELECOMUNICACIONES
MAESTRÍA EN GESTIÓN DE PROYECTOS INFORMÁTICOS

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE MAGISTER EN GESTIÓN DE PROYECTOS INFORMÁTICOS

TÍTULO:

METODOLOGÍA PARA LA PREVENCIÓN DE RIESGOS EN EL MANEJO DE LA INFORMACIÓN PERSONAL ALMACENADA EN EL SISTEMA DE INFORMACIÓN ACADÉMICA DE LA UNIVERSIDAD DE PAMPLONA

Autor:

NANCY MARÍA ACEVEDO QUINTANA

Director:

Ph.D. ISABEL CRISTINA SATIZÁBAL ECHAVARRÍA

PAMPLONA-COLOMBIA

JUNIO de 2016

UNIVERSIDAD DE PAMPLONA
FACULTAD DE INGENIERÍAS Y ARQUITECTURA
DEPARTAMENTO DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, SISTEMAS Y TELECOMUNICACIONES
MAESTRÍA EN GESTIÓN DE PROYECTOS INFORMÁTICOS

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE MAGISTER EN GESTIÓN DE PROYECTOS INFORMÁTICOS

TÍTULO:

METODOLOGÍA PARA LA PREVENCIÓN DE RIESGOS EN EL MANEJO DE LA INFORMACIÓN PERSONAL ALMACENADA EN EL SISTEMA DE INFORMACIÓN ACADÉMICA DE LA UNIVERSIDAD DE PAMPLONA

Autor:

NANCY MARÍA ACEVEDO QUINTANA

Director:

Ph.D. ISABEL CRISTINA SATIZÁBAL ECHAVARRÍA

Codirector
Mg. LUIS ALBERTO ESTEBAN VILLAMIZAR

JURADO CALIFICADOR:
Ph.D. LAURA VILLAMIZAR
Ph.D. JOSE ORLANDO MALDONADO BAUTISTA
M.Sc JOSÉ DEL CARMEN SANTIAGO GUEVARA

PAMPLONA-COLOMBIA

JUNIO de 2016

AGRADECIMIENTOS

A Dios todo poderoso y dador de mi vida

A mi mamá María del Pilar y mi hijo Juan Esteban por llenar mi vida de colores, en momentos que ya no creo poder continuar.

A mi Directora de Tesis, mi amiga Cristina, por su esfuerzo, dedicación, paciencia, sus horarios su forma de trabajar y la motivación han sido fundamentales para mi formación como investigadora

A mi Universidad de Pamplona en cabeza de todos sus profesores que desde varios años me ha ayudado a formarme como persona e investigadora

RESUMEN

El uso eficiente de las tecnologías de la información se ha convertido en un factor de éxito crítico para la sociedad actual. Uno de los aspectos más descuidados es el manejo adecuado de la información personal. Aunque los sistemas de información académica ayudan a tener acceso a la información fácil y rápidamente, también permiten que esta se vea expuesta a diferentes amenazas, más cuando las personas desconocen su importante rol en la cadena de la seguridad. ACADEMUSOFT, el sistema de información académica de la Universidad de Pamplona, no es ajeno a esta realidad, por lo que en este proyecto se diseñó la Metodología de Prevención de Riesgos para Sistemas de Información Académica (MePRiSIA) con el fin de identificar los riesgos a que está expuesta la información personal manejada por este tipo de sistemas y proponer estrategias que permitan prevenirlos y mitigarlos. Esta metodología se compone de 4 pasos: establecimiento del contexto, identificación de riesgos, análisis de riesgos y prevención de riesgos. Para definir MePRiSIA se elaboró primero un estado del arte y una comparación de las metodologías de gestión y prevención de riesgos encontradas en la literatura.

MePRiSIA fue evaluada por 3 expertos, a través una rúbrica y el método Delphi, quienes determinaron que es fácil de entender e incluye el factor humano, pero su implementación es difícil cuando la institución no asigna recursos suficientes para llevarla a cabo. Además, MePRiSIA fue aplicada en el sistema de información académica de la Universidad de Pamplona, donde se evidenció que los mayores riesgos son ocasionados por la falta de políticas, su difusión y, la falta de capacitación y concientización de los docentes, el personal del CIADTI y los estudiantes en seguridad.

ABSTRACT

The efficient use of information technologies has become a critical success factor for today's society. One of the most neglected aspects is the proper handling of personal information. Although academic information systems help to access the information quickly and easily, also they allow that information can be exposed to different threats, particularly when people don´t know their important role in the security chain. ACADEMUSOFT, the academic information system of Pamplona University, is no divorced from reality, so in this project a Risk Prevention Methodology for Academic Information Systems (MePRiSIA) was designed in order to identify risks which personal information, handled by these systems, is exposed and to propose strategies to prevent and mitigate them. This methodology consists of four steps: establishing the context, risk identification, risk analysis and risk prevention. To define MePRiSIA was first developed a state of the art and a comparison of management and risk prevention methodologies found in the literature.

MePRiSIA was evaluated by 3 experts, through a rubric and the Delphi method, who determined that it is easy to understand and includes the human factor, but its implementation is difficult when the institution does not allocate sufficient resources to carry it out. In addition, MePRiSIA was applied in the academic information system of Pamplona University, where it was shown that the greatest risks are caused by the lack of policies, their dissemination and the lack of training and awareness in security of teachers, CIADTI staff and students.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

1 INTRODUCCIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA Y JUSTIFICACIÓN

Internet ha cambiado la forma en que las personas trabajan, se comunican y socializan, por lo que el enfoque y la naturaleza de los sistemas de información y la forma en que estos operan también han cambiado. El uso eficiente de las tecnologías de la información se ha convertido, entonces, en un factor de éxito crítico para la sociedad actual. Sin embargo, la mayoría de las fallas no se deben a la tecnología en sí sino a cómo se usa (Yu, 2004). Uno de los aspectos más descuidados es el manejo adecuado de la información personal. En la ley 1581 de 2012 se define dato personal como: *"cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"*. . Dentro de los datos personales que se utilizan para acceder a un sistema de información está la contraseña, que muchas veces no cumple con la longitud y complejidad recomendadas, pues las personas prefieren elegir contraseñas que sean fáciles de recordar. Además, algunos usuarios revelan sus contraseñas a otras personas, práctica que debe evitarse por seguridad. Por esta razón, los usuarios suelen considerarse el eslabón más débil en la cadena de la seguridad. El artículo "El Ser Humano Factor Clave de la Seguridad" concluye que: "la falta de conocimiento en gestión segura de la información, hace vulnerable al recurso humano de las organizaciones. Debido al componente subjetivo en el comportamiento del ser humano, éste se convierte en un factor vulnerable para la seguridad de la información; por tal razón se debe aprovechar este factor en beneficio de las organizaciones capacitando e instruyendo en las buenas prácticas del manejo de la información." (Lizarazo Rueda, 2012)

La Universidad de Pamplona cuenta con los siguientes sistemas de información (Plataforma, s.f.):

- **Academusoft:** Permite el ingreso, organización, gestión y visualización de la información de los procesos Académicos.

- **Gestasoft**: Permite administrar cuentas, gestionar información financiera de proveedores y clientes, ordenar datos de inventarios, distribución y logística, facilitando el manejo administrativo y financiero de la Institución.

En Academusoft se almacena el historial académico de los estudiantes (notas), sus horarios, datos personales de los estudiantes y docentes, etc. Esta información es de carácter privado y sólo puede ser modificada y visualizada por determinadas personas. Por ejemplo, las notas de una materia sólo pueden ser modificadas por el docente de dicha materia y cada estudiante sólo puede visualizar sus notas. Por ello, se debe proteger celosamente la confidencialidad e integridad de esta información.

Los sistemas de información, aunque ayudan a tener acceso a la información en tiempo real, también permiten que esta se vea expuesta a diferentes amenazas. Por ejemplo, la Universidad de Pamplona ha sido objeto de múltiples denuncias por cambio de notas. Noticias Uno, en octubre de

2013, presentó la noticia: "Investigan venta de notas y títulos profesionales en Universidad de Pamplona" e informó que se descubrió, en la Universidad de Pamplona, un eventual tráfico de calificaciones, inclusive a espaldas de los profesores. Juan Pablo Zapata, estudiante de Unipamplona afirma "No hemos visto, de pronto, que docentes hayan sido sancionados por el cambio de notas y venta de títulos profesionales en la Universidad". Uno de los casos que conoció el noticiero fue el registro de notas del estudiante Salguero Ávila Juan Manuel en donde aparece una nota en cálculo integral de 3.5; el periodista afirma que luego de hablar con la docente de esta asignatura esta dijo: "El joven Juan Manuel Salguero no se presentó durante el semestre, su nota es de (0.0), la calificación que aparece no la doy yo". Además de la mala imagen a nivel nacional que obtuvo la Universidad, según la anterior entrevista, Nelcy Yolima Requiniva Gutierrez, Directora de la Oficina de Control Interno Disciplinario, dijo que varios estudiantes aceptaron haber pagado para obtener el diploma profesional, declaraciones que fueron remitidas a la fiscalía (Tapias, 2013). Esto evidencia que existen personas no autorizadas que están manipulando el sistema de información académica a su antojo y que son personas que pueden haber encontrado un agujero de seguridad en el sistema o a las que se les han dado privilegios sobre el sistema que no les corresponden, lo que implicaría no solo a los estudiantes y profesores en estos sucesos sino también a los encargados de administrar el sistema. Este problema debe, por tanto, ser abordado desde los diferentes puntos de vista de los usuarios del sistema, identificando los roles que tiene cada uno en el sistema, los privilegios asignados de acuerdo a su rol y la información personal que cada uno tiene a su cargo.

Por tal razón, es de vital importancia el diseño de una metodología que permita identificar los riesgos y concientizar a los docentes, estudiantes y administrativos para el uso de buenas prácticas en el manejo de la información personal almacenada en el sistema de información académica de la Universidad de Pamplona.

Así, la pregunta de investigación de este proyecto es: ¿Qué metodología se debería diseñar e implantar para prevenir los riesgos que se presentan en el manejo de la información personal almacenada en el sistema de información académica de la Universidad de Pamplona?.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

Definir una metodología que permita prevenir los riesgos que se presentan al manejar de manera inadecuada la información personal almacenada en el sistema de información académica de la Universidad de Pamplona, lo que contribuirá a fortalecer la seguridad de este sistema y a concientizar a los usuarios sobre la importancia que tienen en la cadena de la seguridad.

1.2.2 OBJETIVOS ESPECIFICOS

- Elaborar el estado del arte de las metodologías de prevención de riesgos existentes, a través de la recopilación y análisis de la información, obtenida por medio de libros, revistas, páginas

web, videos, etc., para poder aplicar este conocimiento en el desarrollo de una metodología que contribuya al uso adecuado de la información personal.

- Diseñar una metodología para la prevención de riesgos en el manejo de la información personal almacenada en el sistema de información académica de la Universidad de Pamplona, basada en los problemas que se presentan actualmente en este sistema y en el estado del arte realizado, para que los usuarios aprendan a proteger adecuadamente la información personal.

- Validar la metodología la metodología de prevención de riesgos en el manejo de la información personal almacenada en el sistema de información académica de la Universidad de Pamplona, a través de la opinión de expertos, para determinar si se ajusta a las condiciones del entorno para la que fue diseñada

1.3 PUBLICACIONES

Se publicó el artículo titulado: *Risk Management and Prevention Methodologies: A Comparison*, en la revista Sistemas & Telemática volumen 14 número 36 de 2016, de la Universidad ICESI (Cali), categoría C en Colciencias (ver Anexo A).

2 MARCO TEÓRICO

2.1 DEFENSA EN PROFUNDIDAD

Para que las empresas puedan defenderse de las diferentes amenazas tanto internas como externas, no basta con aplicar una sola contramedida sino que hay que aplicar un conjunto de ellas, que en conjunto ayuden cubrir las debilidades y protejan a la red interna de los posibles ataques.

El modelo de Defensa en Profundidad ayuda en este propósito y se conforma de 7 capas, en las que se deben instaurar contramedidas. Dichas capas se muestran en la Figura 1 y a continuación se explica cada una (Álvarez Marañón & Pérez García, 2004):

Figura 1. Capas del Modelo de Defensa en Profundidad
Fuente: Seguridad Informática para Empresa y Particulares (Álvarez Marañón & Pérez García, 2004)

- **Capa 1 - Políticas y Procedimientos:** Es quizás la capa más descuidada, pero a la vez la más importante, puesto que las políticas y procedimientos sirven de guía para implantar las otras defensas. Sin embargo, muchas empresas suelen implantar medidas de seguridad a medida que se van presentando los incidentes y no cuentan con unas políticas claras donde se defina cuáles son los activos más importantes para la empresa y qué nivel de seguridad debería tener cada uno. Estas políticas deben ir firmadas por la alta gerencia y deberían darse a conocer a todos los empleados de la empresa y usuarios de la red.
- **Capa 2 – Seguridad Física:** Ya que un atacante podría dañar o robar los dispositivos de la red con toda la información que estos contienen es necesario instaurar medidas de seguridad

física, como: controlar el personal que accede a los distintos recursos y dependencias, instalar sistemas de alarmas, video vigilancia, rejas, etc.

- **Capa 3 – Defensa Perimetral:** El perímetro de una red son aquellos puntos de la red interna, gestionados por la propia organización, que están en contacto con redes externas no fiables. Para defender el perímetro, comúnmente: se instalan cortafuegos (*firewalls*), se utilizan redes privadas virtuales (VPNs), se configuran los *routers* frontera para que no dejen pasar tráfico indeseado, etc.

- **Capa 4 – Defensa de Red:** Aún con las medidas instaladas en las otras capas, un atacante podría tener acceso a la red interna, por lo que se deben instaurar medidas para protegerla. Entre las medidas utilizadas están: sistemas de prevención o detección de intrusos, segmentación de redes, uso de los protocolos IPSec y/o SSL (*Secure Socket Layer*) para el transporte cifrado de datos, protección de redes inalámbricas, etc.

- **Capa 5 – Defensa de Equipos:** Para evitar que un atacante pueda tener acceso a alguno de los equipos a través de la red, estos también deberían estar protegidos, especialmente si se trata de los servidores. La protección de los equipos consiste básicamente en tres tareas fundamentales: actualizar los parches de seguridad, desactivar los servicios innecesarios y mantener activado y actualizado el antivirus.

- **Capa 6 – Defensa de Aplicaciones:** Si un atacante logra entrar al equipo, las aplicaciones deberían estar protegidas. Para ello se puede realizar algún tipo de control de acceso a ellas a través de mecanismos de autenticación y autorización, e instalar cortafuegos de aplicación, para darse cuenta que información reciben y envían a la red.

- **Capa 7 – Defensa de Datos:** Si el atacante pasa todas las defensas anteriores, es necesario que los datos almacenados en el equipo estén protegidos, esto a través de mecanismos de cifrado e integridad.

Además, cada una de estas capas involucra los tres elementos constituyentes de la defensa en profundidad: personas, tecnologías y operaciones. Debe hacer un equilibrio entre estos tres elementos para que las contramedidas implantadas sean efectivas (Álvarez Marañón & Pérez García, 2004):

- **Personas:** Primero que todo, la dirección de la empresa debe concientizarse de la necesidad de asegurar la información, y debe promover la adopción de las políticas y procedimientos de seguridad establecidos, asignar funciones y responsabilidades a los encargados de los activos, y realizar jornadas de formación y concientización del personal (administrativos y usuarios). Además, se deben realizar auditorías periódicas para supervisar las acciones realizadas por el personal e implantar diferentes mecanismos de seguridad física.

- **Tecnologías:** Con base en las políticas y procedimientos de seguridad establecidos se puede determinar qué tecnología es la más adecuada para las necesidades de la empresa. Sin

embargo, implantar tecnologías sin tener un sistema global de gestión de seguridad resulta ineficaz y puede producir una falsa sensación de seguridad que llevaría a defraudar las expectativas de todos los usuarios de la red.

- **Operaciones:** Se requieren acciones diarias como: mantener actualizadas y comunicadas las políticas de seguridad, gestionar la seguridad a nivel tecnológico, evaluar la seguridad de las soluciones implantadas (auditorías y pruebas periódicas), mantener al día el plan de continuidad del negocio y el plan de recuperación ante desastres, actualizar los antivirus, etc.

3 METODOLOGÍA DE INVESTIGACIÓN

Cuando se trata el tema del riesgo en diferentes ámbitos se aborda desde dos perspectivas: la científica y la administrativa. En la científica se hace énfasis en las probabilidades y el punto de vista administrativo se orienta hacia la protección (Gómez Fernández, 2003). Para la realización de la metodología de prevención de riesgos se adopta un enfoque de investigación mixta que permite utilizar técnicas y métodos de las diferentes disciplinas, con el propósito de describir situaciones, eventos y hechos, es decir, cómo es y cómo se manifiesta determinado fenómeno, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis .

El enfoque de investigación mixto permite(Greene, 2007) (Tashakkori & Teddlie, 2008) (Hernández Sampieri & Mendoza, 2008):

- Lograr afinidad o no entre los métodos cuantitativos y cualitativos.
- Un mayor entendimiento de los resultados de un método sobre la base de los resultados del otro método.
- La concepción de cada realidad mediante el abordaje completo e integral de cada fenómeno estudiado, utilizando la información cualitativa y cuantitativa (la visión completa es más significativa que la de cada uno de sus componentes)
- El uso de resultados de un método para ayudar a desplegar el otro método en diversas cuestiones, como: el muestreo, los procedimientos, la recolección y el análisis de los datos, incluso un enfoque puede proveer al otro de hipótesis y soporte empírico.
- Extender la amplitud y el rango de la indagación usando diferentes métodos para distintas etapas del proceso investigativo. Un método puede ampliar el conocimiento obtenido del otro.
- La visualización entre métodos que posibilita que las debilidades de cada uno puedan ser subsanadas por su “contraparte”.
- Pluralidad entre los puntos de vista, incluso divergentes, del fenómeno del planteamiento bajo estudio. Distintas ópticas para estudiar un problema.

3.1 DISEÑO DE LA INVESTIGACIÓN

Para cumplir con los objetivos definidos previamente, el proyecto se ha dividido en 5 fases, basadas en (Lara Ruiz, 2013):

- **Fase 1: Elaboración del estado del arte:** En esta fase se definieron primero los conceptos de prevención y de riesgo, para lo cual se reunió información sobre la prevención en diferentes contextos (democrático, salud, social, educación, redes computacionales) y se determinó

cómo ha evolucionado el concepto de riesgo. Posteriormente, se buscó información sobre el análisis y la gestión de riesgos, para definir la prevención de riesgos en nuestro contexto. Luego, se investigó qué es la gestión de información para definir en qué consiste el manejo de la información personal. La exploración de todos estos conceptos llevó a la definición de metodología de prevención de riesgos. Finalmente, se describieron las metodologías de gestión y de prevención de riesgos encontradas en la literatura, se analizaron, se extrajeron sus fases características y se compararon entre sí.

- **Fase 2: Identificación de los factores de riesgo:** En esta fase se realizó un análisis del sistema de información académica de la Universidad de Pamplona, con el fin de determinar las posibles vulnerabilidades y amenazas que pueden afectar sus activos. Para ello, se identificaron los activos que conforman el sistema y se pidió permiso al CIADTI para explorar los diferentes privilegios de los usuarios del sistema, a fin de determinar su alcance. El CIADTI concedió el acceso a su plataforma de prueba para realizar la exploración del árbol de privilegios. Además, se identificó a qué información personal tienen acceso los estudiantes y docentes a través del sistema de información académica y se les realizaron encuestas para determinar si manejan adecuadamente dicha información.

  Para calcular el tamaño de la muestra de los estudiantes y docentes a encuestar en cada una de las siete facultades, se utilizó la ecuación (1) e información brindada por la Oficina de Planeación sobre el número de estudiantes y docentes en modalidad presencial. El tipo de muestreo realizado fue el aleatorio estratificad.

$$n = \frac{N Z^2 pq}{(N-1)E^2 + Z^2 pq} \quad (1)$$

  Dónde:

  n = Tamaño de la muestra

  N= Tamaño de la población
  Z= Valor estandarizado (1,96)
  p= Probabilidad de ocurrencia (0,5)
  q= Probabilidad de no ocurrencia (0,5)
  E= Error de estimación (0,05)

  Según la Oficina de Planeación, el número total de docentes a nivel presencial, en Pamplona, en el semestre 2015 – II era 1283, por lo que al aplicar la ecuación (1), el tamaño mínimo de la muestra fue N = 296. Luego, se hizo la estratificación y se determinó, según el número de docentes en cada facultad, qué porcentaje de esta muestra corresponde a cada facultad (ver Tabla 1).

Tabla 1. Estratificación Docentes

FACULTAD	Nº DOCENTES	PORCENTAJE	(*ni*)	Nº DOCENTES A APLICAR ENCUESTA POR FACULTAD.
Educación	150	150/1283=0,116*100= 11,69%	11,69%*296 = 34,6	35
Ingeniería y Arquitectura	278	278/1283=0,216*100= 21,67%	21,67%*296=64,14	64
Artes y Humanidades	182	182/1283=0,14*100= 14,18%	14,18% *296= 41,97	42
Salud.	363	363/1283=0,282*100= 28,29%	28,29%*296=83,73	84
Ciencias Básicas	175	175/1283=0,136*100= 13,64%	13,64% *296= 40,37	40
Ciencias Económicas	78	78/1283=0,060*100= 6,08%	6,08%*296= 17,99	18
Ciencias Agrarias	57	57/1283=0,044*100= 4,44%	4,44%*296 = 13,14	13
TOTAL	1283			296

Según la Oficina de Planeación, el número total de estudiantes a nivel presencial, en Pamplona, en el semestre 2015 – II era 10953, por lo que al aplicar la ecuación (1), el tamaño mínimo de la muestra fue N = 371. Luego, se hizo la estratificación y se determinó, según el número de estudiantes en cada facultad, qué porcentaje de esta muestra corresponde a cada facultad (ver Tabla 2)

Tabla 2. Estratificación Estudiantes

FACULTAD	Nº ESTUDIANTES	PORCENTAJE	(*ni*)	Nº ESTUDIANTES A APLICAR ENCUESTA POR FACULTAD.
Educación	1032	1032⁄10953*100= 9,42%	9,42%*371=34,95	35
Ingeniería y Arquitectura	3949	3949⁄10953*100= 36,05%	36,05%*371=133,74	134
Artes y Humanidades	1064	1064⁄10953*100= 9,71%	9,71%*371=36,02	36

FACULTAD	Nº ESTUDIANTES	PORCENTAJE	(*ni*)	Nº ESTUDIANTES A APLICAR ENCUESTA POR FACULTAD.
Salud.	3079	3079/10953*100= 28,11%	28,11%*371=104,29	104
Ciencias Básicas	491	491/10953*100= 4,48%	4,4%* 371=16,32	17
Ciencias Económicas	658	658/10953*100=6%	6%* 371=22,26	22
Ciencias Agrarias	680	680/10953*100= 6,21%	6,21%*371=23,04	23
TOTAL	10.953			371

La encuesta realizada a los docentes contiene 13 preguntas de selección múltiple y la encuesta realizada a los estudiantes contiene 11 preguntas de selección múltiple. En el Anexo B se encuentran los resultados de dichas encuestas.

- **Fase 3: Diseño de la metodología:** Para diseñar la Metodología de Prevención de Riesgos para Sistemas de Información Académica (MePRiSIA) se tomaron como referencia las metodologías exploradas en el estado del arte y se determinaron las características que iban a diferenciar esta nueva metodología de las existentes. A partir de ello, se establecieron el propósito y los objetivos de la metodología así como el público objetivo. Los pasos de MePRiSIA son las fases que se extrajeron para la comparación de las metodologías en el estado del arte. Luego, se revisó la forma en que las diferentes metodologías llevaban a cabo las fases establecidas y se determinó qué era lo más importante de cada fase y cuál sería la forma más sencilla de obtener el resultado esperado. De esta manera se establecieron los 3 primeros pasos de MePRiSIA.

  En el paso 4 de la metodología, se combinaron las vulnerabilidades identificadas en los activos del sistema de información académica de la Universidad de Pamplona, los 4 elementos de la Metodología de Gestión de Incidentes de Malware según NIST (Mell, Kent, & Nusbaum, 2005), el modelo de defensa en profundidad (Álvarez Marañón & Pérez García, 2004) y el conocimiento del director de este proyecto sobre las contramedidas de seguridad, para definirlo.

- **Fase 4: Evaluación de la metodología:** Para evaluar la metodología se eligió un grupo de 3 expertos: dos externos y uno interno, se elaboró una rúbrica para que evaluaran las características distintivas de la metodología en los diferentes pasos y se utilizó el método

Delphi para determinar si había consenso en sus opiniones. Además, se aplicaron los pasos de la metodología al Sistema de Información Académica de la Universidad de Pamplona (ACADEMUSOFT).

- **Fase 5: Análisis de los resultados y elaboración del informe:** En esta fase se analizaron los resultados de las evaluaciones de los expertos como de la aplicación de la metodología a ACADEMUSOFT, y se realizaron los cambios que se consideraron pertinentes en la metodología. Fue necesario explicar mejor el paso 2 de MePRiSIA y, redefinir y completar las contramedidas del paso 4.

En la Figura 2 se presenta un resumen de las actividades desarrolladas en cada fase para alcanzar los objetivos propuestos.

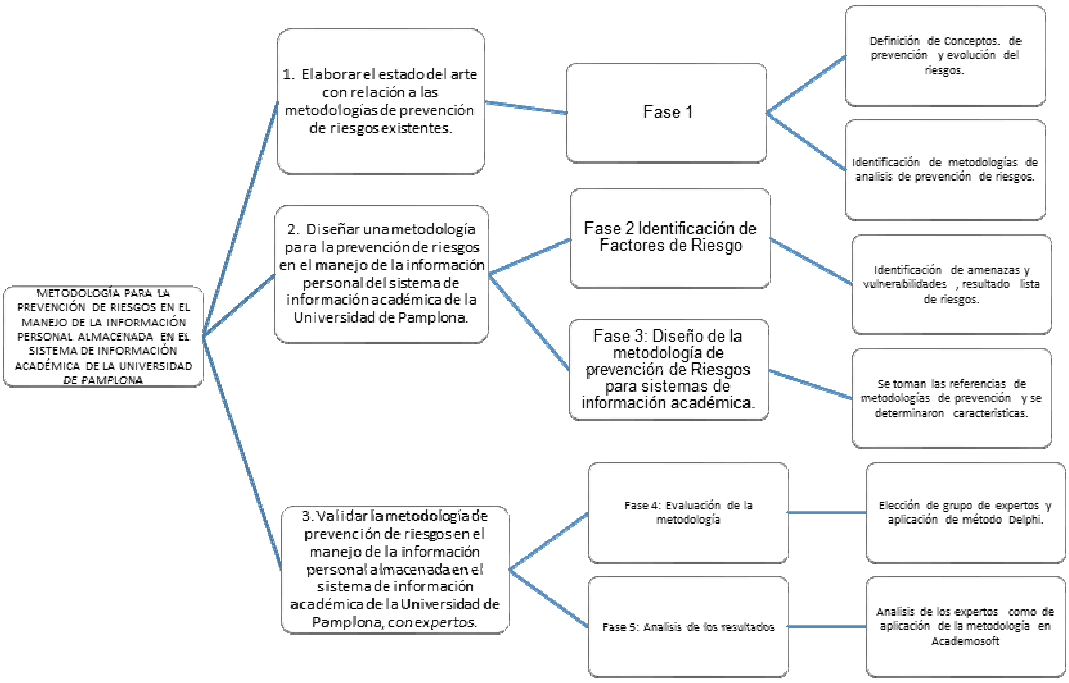

Figura 2. Actividades Desarrolladas en Cada Fase

4 ESTADO DEL ARTE

4.1 CONCEPTO DE PREVENCIÓN

4.1.1 PREVENCIÓN A NIVEL DEMOCRÁTICO

A nivel democrático se utiliza el concepto de prevención de conflictos. La prevención de conflictos ganó gran atención después de la Guerra Fría, debido a la concientización que hubo sobre los peligros que acarrea la guerra intra-estatal y el colapso de los estados, llevando a intervenciones complejas en conflictos violentos y al crecimiento de la presión pública para que se prevengan los genocidios y los conflictos (International_Commission_on_Intervention_and_State_Sovereignty(ICISS), 2001).

Las estrategias de prevención de conflictos se pueden dividir en dos categorías: prevención estructural y prevención directa u operacional (Wallensteen, 2002b). La prevención estructural incorpora medidas para asegurar que la crisis no surja, en primer lugar, y si lo hace, que no se repita. La prevención operacional o directa consta de medidas aplicables para enfrentar crisis inmediatas(Carnegie_Commission_on_Preventing_Deadly_Conflict, 1997) . La elección entre prevención estructural o directa depende de las áreas de desacuerdo, el tiempo apropiado para implantar la acción de prevención, los niveles en que las medidas preventivas deben ser aplicadas, así como de las diferentes teorías sobre las causas de los conflictos y cómo estos deben ser tratados. La perspectiva a largo plazo de la prevención estructural incluye temas como la democracia, la buena gobernanza, las normas internacionales, los tribunales internacionales, el fortalecimiento de organizaciones internacionales y la reducción de la pobreza. El desarrollo de sistemas de alerta y respuesta temprana, sanciones económicas y el uso de la fuerza, son medidas de prevención directa de conflictos, una perspectiva a corto plazo.

La democracia es incluida en las definiciones de prevención estructural de conflictos pues proporciona a las comunidades ,o grupos de personas contendores, la posibilidad de resolver las diferencias de manera pacífica a través del sistema político, en lugar de promover la violencia (Byman, 2003). Por tanto, es casi imposible distinguir entre la promoción de la democracia y la prevención de conflictos (Olsen, 2002). Estratégicamente, la prevención estructural ofrece una importante oportunidad de promover reformas en la sociedad tendientes a la democracia (Wallensteen, 2002a).

La Organización de Estados Ameircanos (OEA) se enfoca en la democracia como un mecanismo para la prevención de conflictos, a través de su Unidad para la Promoción de la Democracia (UPD), y los Estados Unidos buscan promover la democracia como medio para alcanzar la seguridad, estabilidad y prosperidad en todo el mundo (U.S._Department_of_State).

El uso vago del término democracia, cuando se discuten las estrategias preventivas, es problemático. La democracia y los derechos humanos, dos de los principales ingredientes de las

estrategias de prevención estructural, son entendidos comúnmente como dos caras de la misma moneda (Boutros-Ghali, 1996) (Boutros-Ghali, 1995).

Michael Lund ofrece una definición amplia y completa de la prevención de conflictos como: "cualquier medio estructural o intercesor que previene que las tensiones y disputas intra-estatales e inter-estatales se transformen en violencia significativa y uso de la fuerza armada, fortaleciendo las capacidades de las posibles partes del conflicto violento para resolver tales disputas pacíficamente y para reducir progresivamente los problemas subyacentes que producen dichas disputas" (Lund, 2001) . Dress y Rosenblum-Kumar argumentan que cuando las Naciones Unidas y la comunidad internacional usan el término "prevención de conflictos", lo que quieren decir es "prevención de la violencia" (Rosenblum-Kumar). Ellos están de acuerdo con Lund y exigen un enfoque amplio e integral para la prevención de conflictos que se ocupe de las injusticias estructurales, la pobreza y la desigualdad horizontal, así como de las crisis inmediatas. Stephen John Stedman dice que la ausencia de intereses bien definidos, metas claras y un juicio prudente sobre los costos y riesgos aceptables, las políticas de diplomacia preventiva y la prevención de conflictos, simplemente significa que se llegue más temprano que tarde a una crisis (Stedman, 1995).

La vaguedad del término prevención de conflictos no solo oscurece el debate académico, sino que obstruye la necesidad de pasar de la retórica a la práctica. Para que la prevención sea efectiva se debe saber a qué nos estamos refiriendo cuando usamos el término. Aquellos que desean enfocarse en la prevención estructural ambicionan una normativa clara y los que se enfocan en la prevención directa u operacional buscan ayudar a construir una "mejor" sociedad basada en la paz y la tolerancia. La prevención directa incluye un aspecto normativo en el intento de evitar la violencia inminente y las muertes, sin embargo es demasiado limitado. Muchos científicos involucrados en la discusión sobre prevención tienen un enfoque claramente orientado a las políticas, aunque basado en diferentes fundamentos teóricos. Las experiencias negativas de las Naciones Unidas y de otros actores internacionales en Croacia 1991-1992, Bosnia-Herzegovina 1992-1995, Somalia 1992-1993 y Ruanda 1994 han motivado muchos de estos. Sin embargo, a pesar de las muchas recomendaciones políticas ofrecidas, muchos las han criticado por ser demasiado generales para ser efectivas (Wallensteen, 1998) (Hampson, 2002).

A principios de los 90s los investigadores empezaron a recopilar información pertinente sobre las políticas de prevención a través de cuantificación, casos de estudio y evaluación de la investigación. Sin embargo, todavía existe confusión sobre la definición y la recomendación de políticas, lo que probablemente contribuye a la dificultad de dirigirse hacia un sistema más efectivo de prevención en la práctica. Muchas de las medidas incluidas en las estrategias preventivas, especialmente en las estrategias de prevención estructural, se basan en ideas liberales (Lindblom, 2003).

4.1.2 PREVENCIÓN EN EL CAMPO DE LA SALUD

El concepto de prevención está ligado al proceso salud-enfermedad. En cada época de la historia se han dado diferentes interpretaciones a la salud y a la enfermedad, las cuales a su vez se relacionan con las situaciones políticas, económicas y sociales de cada momento histórico .

Las primeras prácticas del cuidado surgieron por instinto y la observación de la naturaleza, al aprender de los animales e identificar las circunstancias más evidentes que producían enfermedad.

Dada la división del trabajo por género, fue la mujer la encargada de preservar lo básico para vivir, como la alimentación, la siembra, la domesticación de animales. Por ese conocimiento de la naturaleza surgen las "mujeres sabias", poseedoras de grandes secretos medicinales, verdaderas herbolarias, quienes desempeñaron el rol de cuidadoras de los enfermos.

Las antiguas civilizaciones continuaron con el conocimiento empírico del cuidado, dándose la división entre el cuidar y el curar. El curar, que progresó entre los médicos y la medicina, permitió aportes significativos en el diagnóstico, la clasificación de las enfermedades, el desarrollo de las ciencias biológicas, y trasformó la medicina mágica en científica. El cuidado, mientras tanto, permaneció relegado a la mujer, debido a que aquél se prestaba en el hogar o en comunidades muy restringidas.

La prevención de la enfermedad fue notoria en la India durante los años 2.500 y 1.500 a.C. Los hindúes en el libro Ayurveda, encontraban lo referente a la práctica de cuidado de la salud, en el que se describían las cualidades mínimas de los encargados de la prestación de servicios, resumidos en: conocer la forma en que se debían preparar los medicamentos para su administración, inteligencia, vocación por los enfermos y pureza tanto del cuerpo como de la mente.

En el budismo, durante los años 269 a 263 a.C., el rey Asoka, favoreció la creación de instituciones sociales y de caridad; además estableció normas morales para quienes se dedicaban a curar y cuidar; oficios que necesitaban permiso especial y requisitos tales como: bañarse cuidadosamente por lo menos una vez al día, limpiarse los dientes, baño ocular con colirios[1], cortarse las uñas, usar siempre ropa blanca y limpia, perfumarse y adorar a los dioses. El mismo reglamento imponía tratar a las personas con ternura y suavidad, con la recomendación de guardar el secreto de sus confidencias. Así, la prevención de la enfermedad se consideraba de primordial importancia y el cuidado del cuerpo constituía un deber religioso.

[1] **Colirio:** Medicamento líquido de uso externo que se emplea para curar o aliviar las enfermedades de los ojos (http://www.wordreference.com/definicion/colirio)

.

Los chinos fieles seguidores de la religión taoísta, se enfocaron hacia la prevención de las enfermedades; como lo observó el padre de la medicina china, Huang Ti: "el mejor médico es el que ayuda antes de que aparezca la enfermedad". Mantenían la salud por medio de la meditación, los ejercicios gimnásticos y respiratorios y el respeto por el otro, lo que constituía un tratado ético-humanístico, o lo que hoy se conoce como conocimiento de sí mismo.

Los hebreos prohibían las prácticas mágicas en el curar y el cuidar; su carácter religioso monoteísta estableció normas higiénicas, más con fines de religión y disciplina, que con el propósito de prevenir enfermedades. Enfatizaron en la importancia de la limpieza del cuerpo, el sueño, la dieta y el reposo sabático como practica de salud. Como prevención de contagio, los leprosos eran aislados de otros miembros de la sociedad, y algunas enfermedades como la difteria debían ser reportadas inmediatamente a las autoridades como norma de protección sanitaria.

Los egipcios antiguos prestaron especial atención a la limpieza del cuerpo y de sus casas. Cada mes empleaban purgantes, enemas y vomitivos como símbolo de purificación interna para liberar los *metu*[2] del peligroso contenido intestinal; esta práctica era realizada para prevenir enfermedades.

En Grecia, a mediados del siglo IX a.C., los dioses actuaban como causales de enfermedad, y al tiempo, como agentes de curación y prevención. Asclepio fue la personificación del supremo sanador, su esposa Epione, fue conocida como la que reconforta; y una de sus hijas, Higea, la diosa de la salud, más tarde pasó a simbolizar la prevención. Al dios Asclepio le construyeron templos de la salud que conjugaban las funciones de santuarios religiosos y balnearios medicinales.

En la época de los filósofos científicos se creyó que el equilibrio entre los cuatro elementos; agua, tierra, fuego y aire, prevenía las enfermedades; sin descuidar las recomendaciones sobre la dieta, la meditación, el ejercicio y la música.

Con Hipócrates se dio la medicina racional, entre sus aportes se destacó la concepción de que la enfermedad no era obra de espíritus, dioses o demonios; sino consecuencia de transgredir las leyes naturales. La constante que se manifestó en todos los tratamientos hipocráticos, era la confianza en la naturaleza para conseguir y mantener la salud.

Los romanos tomaron de los griegos las prácticas de prevención, cuidado y restauración de la salud, lo cual unido a los elementos de construcción que poseían: desagües, suministros de agua, calles pavimentadas, casas bien construidas y baños públicos; contribuyó a mantener un adecuado régimen sanitario. La alta consideración por las técnicas agrícolas, los llevo a establecer normas dietéticas saludables, elementos que favorecían el cuidado de la salud.

Galeno, médico romano que vivió del 129 al 200 d.C., concedió especial importancia a la prevención de las enfermedades mediante regímenes higiénicos, que ayudaban a la naturaleza en su función, con especial énfasis en el descanso y en el ejercicio.

[2] Según su creencia el cuerpo estaba constituido por canales llamados *metu,* cuyo centro era el corazón.

En los siglos III a V d.C., durante la decadencia del imperio Romano, cobró fuerza el cristianismo. El deseo de imitar a Cristo, dio origen al cuidado de los enfermos y desvalidos, como principio de las obras de misericordia, aun cuando esto se hiciera más para la salvación del que curaba, que la del enfermo. En este sentido, surgió la creencia común de la enfermedad como un castigo por el pecado. Solo la gracia de Dios podía conseguir la curación por lo que se relevaba de esta responsabilidad a aquellos que proporcionaban los cuidados. Esta situación contribuyó al descuido de la prevención de la enfermedad, y se dirigió solo a los aspectos propios del cuidado, por lo que se crearon numerosas instituciones para la atención de los enfermos y desheredados.

La adopción del modelo de hospital militar romano, llevó a la creación de numerosos hospitales cristianos en toda Europa, con la diferencia de que en los militares, no se incluía un cuidado de enfermería prolongado y los hospitales cristianos fueron los primeros en asistir durante largos períodos a los enfermos, pobres y marginados, con cuidados de enfermería sencillos proporcionados a menudo por mujeres de noble cuna.

Se crearon los monasterios donde se congregaban algunas personas para brindar cuidado en nombre de Cristo, sometidos a normas estrictas, convencidos de lograr la curación de la enfermedad mediante la oración. En esta época los avances de la medicina se atrasaron, al considerar el cuerpo impuro y pecaminoso situación que no permitía el contacto físico con el enfermo y el abandono de las prácticas de salud, lo cual se convirtió en factor desencadenante de las epidemias, que diezmaron los pueblos europeos.

La prestación de los servicios de salud cambió hasta finales del siglo XVII, cuando los dirigentes empezaron a darse cuenta que una población sana beneficiaba a los intereses del Estado.(Muñoz Giraldo, 2004).

La prevención fue descrita en 1945 por Henry Sigerist como una de las tres funciones de la medicina, junto con la reparación o tratamiento del daño y la rehabilitación. Más adelante, los norteamericanos las denominaron como funciones de la salud pública.

Sigerist hizo una distinción entre la promoción de la salud y la prevención de la enfermedad, y reconoció que las medidas de la promoción de la salud tienen efectos preventivos y no lo contrario, es decir, un programa para evitar el consumo del cigarrillo se constituye en una actividad de promoción; más uno que apunte a la cesación o reducción de fumar está desarrollando acciones de prevención: el hecho de no fumar está suprimiendo riesgos frente a enfermedades inherentes al cigarrillo.

La prevención tiene que ver con las teorías de causalidad de la enfermedad en cualquier modelo médico; ella ha sido definida como: "La aplicación de medidas técnicas que incluye aspectos médicos y de otras disciplinas que tienen como finalidad impedir la aparición de la enfermedad (prevención primaria), curarla (prevención secundaria) y devolverle las capacidades perdidas (prevención terciaria)"(Ministerio_de_Salud., 1993).

La prevención primaria es: "el conjunto de actividades dirigidas a reducir el riesgo de sufrir enfermedad mediante la disminución del nivel de los factores de riesgo o de la probabilidad de su ocurrencia"; la prevención primaria contempla dos niveles, en el primero propone la "promoción general de la salud" y en el segundo, "la protección específica"; el objetivo de la promoción general, así entendida, plantea la necesidad de: "crear las condiciones más favorables para resistir la enfermedad, aumentar la resistencia y colocarlo en un ambiente favorable a la salud" (Ministerio_de_Salud., 1993); si se analiza este objetivo, se ve como se involucra la presencia de enfermedad, y no el fomento y el cuidado de la salud y de la vida, que es lo primordial de la promoción de la salud (Ministerio_de_Salud., 1993).

El hecho de no tener claridad acerca del concepto de salud y de los modelos teóricos en los cuales se sustenta, por un lado, la promoción y por otro la prevención, genera dificultades en el planteamiento y logro de metas, en la determinación de estrategias, en la claridad frente a los sujetos a quienes van dirigidas las acciones y en la destinación de recursos, entre otros aspectos, que son del ámbito de cada uno de estos enfoques; de aquí que la denominación “promoción y prevención” haya llevado a que en la práctica se privilegien las acciones de prevención sobre las de promoción. Para éstas hay que actuar sobre los determinantes de la salud, lo cual necesita de grandes inversiones, trabajo intersectorial, compromiso político y en definitiva, un replanteamiento de las estructuras del país.

Desde el punto de vista de los sujetos involucrados, la prevención recoge a individuos y grupos sociales específicos, los cuales por sus características son susceptibles de adquirir enfermedades también específicas. Implementar las medidas de prevención por ser precisas, específicas y puntuales genera menos costos y los resultados se dan a corto y mediano plazo, diferente a lo que ocurre en la promoción como un proceso que requiere crear condiciones favorables para la salud y la vida, por lo tanto, sus resultados son a largo plazo.

La participación comunitaria dentro de la prevención está limitada a la ejecución de las acciones y es generalmente impuesta desde niveles superiores (participación prescrita), “el programa hecho por los técnicos contiene elementos que requieren de la participación activa”(Kroeger & Luna, 1992), por ejemplo: la mano de obra de la comunidad, la movilización de líderes, o la utilización de recursos financieros de la comunidad. En este contexto es claro que el responsable de planear las acciones de prevención es el sector salud con apoyo de otros sectores y éstas son desarrolladas por el personal de salud en cooperación con la comunidad .

4.1.3 PREVENCIÓN EN EL CONTEXTO SOCIAL

La prevención desde el contexto social, se identifica a simple vista como acciones que permiten, eliminar o reducir las condiciones de criminalidad presentes en lo social, cuando todavía no se han manifestado señales de peligro, y puede comprender medidas dirigidas a grupos en riesgo delictivo o a un evento criminal que ya ha sido cometido, para prevenir posteriores recaídas (Brantingham & Faust, 1976)

La prevención puede ser entendida, según una de las más recientes definiciones, como: "la interrupción del mecanismo que produce un evento delictivo" (Ekblom, 1996) (Pease, 1997). Tal mecanismo causal puede ser reconducido a tres elementos de fondo: la estructura, la motivación individual y las circunstancias. Lavrakas (Lavrakas, 1995) ha individualizado un esquema en el cual los tres niveles de prevención se entrecruzan con cuatro "contextos operativos": los individuos, las viviendas, el barrio y la sociedad. Este puede llevarse adelante a través de una intervención sobre el contexto, físico y social, sobre las situaciones en que la criminalidad es el resultado de una serie de circunstancias y oportunidades. En la perspectiva estructural, la criminalidad es el producto de condiciones sociales y económicas y la prevención se entiende entonces como la actividad que incide sobre tales causas de fondo. Por otro lado, se entiende el delito como el producto de las preferencias humanas, y la prevención se concentra en la intervención individual, de modo que se debe detener, controlar o rehabilitar a los autores reales o potenciales.

Una definición "nueva" de prevención es: "el conjunto de las estrategias dirigidas a disminuir la frecuencia de ciertos comportamientos, sean estos considerados punibles o no por la ley penal". La diferencia respecto al sistema penal consiste en que, al modelo conceptual pasivo e indirecto de la prevención penal, se contrapone una forma de prevención directa y pro-activa (Robert, 1991). Las políticas de prevención dentro de una organización recalcan componentes de pragmatismo[3i], eclecticismo[4.] y una tendencia al reduccionismo[5] de la complejidad y se borran cada vez más las fronteras entre las políticas preventivas y las otras políticas públicas. Estas se van condicionando por objetivos que no son necesariamente la reducción de la criminalidad, sino el producto del conflicto político y de las exigencias administrativas (Hope, 2002).

En un análisis de los programas preventivos realizados en Bélgica en los años 80, Welgrave y De Cauter (Walgrave & De Cauter, 1986) analizan críticamente una clasificación basada en la distinción entre los momentos en los que interviene la acción preventiva (antes, durante o después del evento indeseado), y el enfoque de la intervención preventiva (los comportamientos de los sujetos o la modificación del contexto social) y la orientación defensiva (sobre los síntomas) u ofensiva (sobre las causas).

[3] **Pragmatismo:** Movimiento filosófico iniciado en los Estados Unidos por C. S. Peirce y W. James a fines del siglo XIX, que busca las consecuencias prácticas del pensamiento y pone el criterio de verdad en su eficacia y valor para la vida (Real_Academia_Española). Actitud y pensamiento que valora sobre todo la utilidad y el valor práctico de las cosas (Wordreference.com).

[4] **Eclecticismo** (De *ecléctico*) Modo de juzgar u obrar que adopta una postura intermedia, en vez de seguir soluciones extremas o bien definidas. Escuela filosófica que procura conciliar las doctrinas que parecen mejores o más verosímiles, aunque procedan de diversos sistemas (Real_Academia_Española).

[5] ***Reduccionismo***: Enfoque filosófico según el cual la reducción es necesaria y suficiente para resolver diversos problemas de conocimiento. (Wikipedia)

Dentro de la prevención social se busca cambiar las motivaciones delictivas que son percibidas como algo que reside en las personas más que en las cosas, el ambiente social. Busca alcanzar esto a través de medidas típicas de la política social como políticas de vivienda, educación y tratamiento sanitario con respecto al alcohol y el delito; política familiar y educativa, trabajo para los jóvenes y políticas de empleo (Gilling, 1997). Entonces la prevención social, no es una acción específica o una de las numerosas modalidades de prevención, sino una política global orientada al bienestar social que atraviesa todos los sectores de las políticas administrativas (Walgrave & De Cauter, 1986) (Peyre, 1986) (Graham & Bennett, 1995) (Knepper, 2007).

Tonry y Farrington (Tonry & Farrington, 1995), rechazan esta visión amplia y con la intención de ser más claros, separan la prevención social en dos partes: una relativa a las motivaciones individuales y la otra relativa al contexto social. De este modo la "prevención social" desaparece y se distingue en las estrategias hacia el autor potencial (la llamada prevención del desarrollo) y en las medidas basadas en la transformación de las condiciones sociales de la comunidad (la llamada prevención comunitaria del delito). Con este tipo de connotaciones surge una nueva visión en cuanto a la "prevención precoz" que se caracteriza por tres elementos distintivos: el primero se refiere a medidas que hay que tomar en una fase temprana de la vida de las personas, y sobre esta precocidad hay discordancia de opiniones, ya que hasta antes del nacimiento de los individuos existirían factores de riesgo ligados a las costumbres y a las condiciones de vida de la madre o de las familias iniciando desde la primera infancia y siguiendo en la adolescencia; en segundo lugar, prevenir el primer acto delictivo en la vida de los individuos; y en tercer lugar la intervención de naturaleza estrictamente social, tanto hacia el individuo, como hacia los grupos sociales y el contexto social en general (Farrington & Welsh, 2007).

Así, la perspectiva de la prevención social es simple: considerando que los comportamientos criminales son el resultado de predisposiciones y oportunidades se intenta modificar las predisposiciones, cuanto sea posible, pasando después a modificar las oportunidades (Savona, 2004).

4.1.4 PREVENCIÓN Y EDUCACIÓN

En los últimos años se ha proclamado frecuentemente que "la prevención comienza con la información". Se trata sin duda de una consigna válida e importante, desde el momento en que resalta la difusión de conocimientos (conceptos básicos, datos relativos al comportamiento de las amenazas, etc.) como factor crucial para la prevención. Sin embargo, así como existen múltiples modos de conocimiento también hay múltiples modos de información.

En la praxis educativa existe un auto-límite que aparece mediante opciones memorísticas y autoritarias, que obstaculizan el crecimiento de potencialidades específicamente humanas, y a su vez estos estilos educativos desmejoran la capacidad de prever, lo cual es esencial para formar una conciencia preventiva (A. Campos, 1999).

Prevenir, según el sentido común, significa actuar con anticipación para evitar que algo ocurra, pero se crean ciertas confusiones a la hora de precisar qué es lo que se quiere evitar, ya que la prevención es una intencionalidad práctica que atraviesa todo el proceso de desastre y que da lugar a diferentes objetivos y acciones en cada una de ellas. Holland y Van Arsdale (Holland & Van Arsdale, 1989) definen que: un desastre constituye para el individuo la demostración amplia de que su cultura y su modo de vida se han vuelto repentinamente inadecuados, incapaces de protegerlo de las vicisitudes del medio ambiente. Sin embargo, es la cultura de cada persona la que gobierna sus interacciones con sus semejantes y con el medio. Cuando ocurre un desastre, muchas de las normas y valores que son parte de una cultura dejan de ser útiles para satisfacer las necesidades que se originan. El desastre altera las percepciones de la sociedad y las reglas que rigen el comportamiento diario. Más aún, muchos especialistas han llegado a sugerir que se desarrolla una "cultura del desastre", que reemplaza provisionalmente las normas y valores vigentes por otros más apropiados para satisfacer la necesidad.

El concepto de prevención incluye un significado de evitación, pero pierde fuerza si se limita a ese alcance. En lo que respecta a las emergencias y los desastres, una determinada acción tendrá contenido preventivo cuando de cualquier forma se encamine a evitar daños y trastornos mayores y, al mismo tiempo, a favorecer condiciones para la recuperación material y psicosocial de los afectados.

Los estudios e iniciativas programáticas en educación preventiva traen consigo la necesidad de conocer y manejar diversos problemas micro-políticos, como los relacionados con los intereses de los educadores o las auto-percepciones de los estudiantes. El resultado de estos estudios permite describir la vulnerabilidad en términos de factores. Por ejemplo, según la Serie 3.000 "se pueden considerar diversos tipos de vulnerabilidad: estructural, social, económica, organizativa, cultural, biológica, sanitaria, ambiental". O, según la sistematización que efectúa Wilches-Chaux, podemos distinguir factores de vulnerabilidad ambientales, físicos, económicos y sociales (Wilches-Chaux, 1998).

La prevención de la violencia en la escuela se compone de dos vertientes: la de la salud pública y la de los derechos.

En el campo de la salud pública, la prevención primaria arranca de un enfoque de riesgo y del diseño de factores protectores. Consiste en bajar la incidencia de los daños y contrarrestar las circunstancias dañinas antes de que se produzca la oportunidad de la violencia. No se trata de prevenir a una persona específica para que no cometa un acto violento, sino más bien de reducir este riesgo en toda una población.

La prevención primaria busca fomentar un ambiente social e individual de respeto y tolerancia, de valores sociales y de conducta personal que favorezcan que los conflictos se resuelvan de maneras no violentas, o sea, se dirigen a evitar que ocurra el hecho violento. Forman parte de este nivel de prevención las estrategias macro destinadas a disminuir la pobreza, a buscar la equidad social, a mejorar la educación y a recuperar la ética y el control social (Concha-EastMan, 2004).

La prevención secundaria busca detener precozmente o retardar el progreso de la violencia o de sus secuelas en cualquier punto de su aparición. Para ello son importantes las medidas de detección precoz en individuos y poblaciones para efectuar una intervención rápida y efectiva al inicio de las manifestaciones (Sánchez, 2004).

La prevención secundaria se aplica cuando un evento violento ya ha ocurrido, y su intención es evitar nuevos episodios o disminuir su gravedad.(Concha-EastMan, 2004).

La prevención terciaria se orienta a reducir las complicaciones y consecuencias de los daños de la violencia, adquiriendo importancia la rehabilitación para mejorar la calidad de vida (Sánchez, 2004).

En el campo de los derechos, un sistema de protección legal se expresa en la defensa y garantía de los derechos de las personas menores de edad en el sistema de justicia. Un sistema de protección social conduce al cumplimiento de los derechos sociales y se extiende desde las políticas universales hasta las políticas focalizadas dirigidas a niños, niñas y adolescentes

Luego la prevención e intervención individual y grupal se afrontan desde la perspectiva colectiva, ampliándose de esta manera en todos los ámbitos. El ejercicio de la ciudadanía, en el que se plantea que ser titular de derechos debe ser sinónimo de poder ejercerlos (Krauskopf, 2006).

Existen variables internas y externas que intervienen en la prevención de la violencia escolar. Las variables internas (endógenas) se refieren a factores que podríamos llamar instrumentales o directos, como los sistemas de normas y reglamentos, así como los proyectos político-pedagógicos (Hayden & Blaya, 2001) (Ragmognino, FradJi, Soldini, & Vergés, 1997). Un ejemplo muy detallado es el que presenta Sinclair, cuando los estudiantes que regresan de largas suspensiones o expulsiones, desde su casa o lugares con medidas de seguridad, se encuentran a menudo en riesgo de fracasar académicamente o desertar del sistema. Por lo general, se encuentran rezagados académicamente como resultado de haberse perdido meses o incluso años de escuela. Con posterioridad a la deserción (salida) de la escuela, muchos estudiantes experimentan una enorme dificultad para volver a ingresar (Sinclair, 1999)

Una segunda variable, la externa, son las habilidades vinculadas a aprender, a ser y convivir, que cubren una amplia gama de capacidades: asumir retos en lo académico; establecer relaciones humanas estables y satisfactorias; mantener la esperanza sobre el futuro; tomar decisiones oportunas, adecuadas, efectivas y constructivas; optimizar el uso de las redes sociales; actuar con solidaridad y sentido social; tener capacidad de resolución general de problemas; aumentar el auto-cuidado, autocontrol, la autorregulación y la autonomía; manejar las tensiones de la vida cotidiana; hacer frente a la presión de los pares; manejar los grandes volúmenes de información; la capacidad para transformarse a sí mismo y transformar su entorno (Krauskopf, 2006).

Díaz dice que la prevención en el contexto educativo debe fortalecer cuatro capacidades fundamentales: permitir al alumno establecer vínculos de calidad en diversos contextos; ser eficaz en situaciones de estudio-trabajo, movilizando la energía y el esfuerzo precisos para ello, y

obteniendo el reconocimiento social necesario; integrarse en grupos de iguales constructivos, resistiendo presiones inadecuadas; y desarrollar una identidad propia y diferenciada que le ayude a encontrar su lugar en el mundo y le permita apropiarse de su futuro .

4.1.5 PREVENCIÓN EN LAS REDES COMPUTACIONALES

En la seguridad en redes, la prevención significa mantener a los atacantes alejados (es decir, prevenir que los atacantes entren a la red) (Khan Pathan, 2010). Es así como se habla de la prevención de ciber-crímenes, prevención de incidentes y prevención de intrusos.

Todos los productos existentes en el mercado de la seguridad informática cumplen una función entre las siguientes :

- **Prevenir:** Aumentan el nivel de seguridad evitando que los ataques tengan éxito. El ejemplo clásico es el cortafuegos

- **Detectar:** Se encargan de velar por que todo esté en orden y de alertar cuando se produce una anomalía, normalmente debida a un intruso. Un ejemplo típico es un sistema de detección de intrusos o IDS

- **Recuperar:** Garantizan que ante un incidente de seguridad, causado o fortuito, se pueda recuperar toda la información y retornar a la normalidad en un tiempo mínimo. El ejemplo más conocido lo constituyen las copias de seguridad.

Estos tres pilares se realimentan unos a otros: la prevención evita tener que recurrir a la recuperación, mientras que la detección facilita la recuperación y realimenta la prevención. Para que un sistema sea razonablemente seguro, deben implantarse los tres tipos de medidas coordinadamente .

La prevención del crimen, en el contexto del ciberespacio, significa reducir el riesgo de ocurrencia del crimen y la gravedad potencial del crimen y de eventos desordenados, que pueden ocurrir tanto en línea como fuera de línea (Ekblom, 2003). Para lograr esto, es necesario identificar los problemas y sus causas, pero dado el desarrollo reciente y rápido del ciberespacio no es sorprendente que exista mucha incertidumbre sobre los problemas futuros que surgirán y cómo deberán ser tratados (Collins & Mansell, 2004) .

En la prevención de incidentes, por otra parte, existen cuatro elementos principales: políticas, concientización, mitigación de vulnerabilidades y mitigación de amenazas. Las políticas son la base para implementar controles preventivos. Los programas de concientización para todos los usuarios, así como los programas de entrenamiento específico en concientización para el personal de TI directamente involucrado en las actividades de prevención de incidentes, son críticos para reducir el número de incidentes que ocurren por errores humanos. Invertir esfuerzo en la mitigación de vulnerabilidades puede eliminar algunos posibles vectores de ataque. Implementar una combinación de técnicas y herramientas de mitigación de amenazas puede prevenir que las

amenazas de diferentes sistemas y redes atacantes sean exitosas. Sin embargo, las organizaciones deben ser conscientes de que no importa cuánto esfuerzo pongan en la prevención de incidentes, los incidentes todavía ocurrirán (Mell et al., 2005).

Un sistema de prevención de intrusos o IPS (*Intrusion Prevention System*), es un dispositivo o programa utilizado para detectar señales de intrusión en las redes o sistemas y tomar una acción. Dicha acción consiste en generar alarmas y/o bloquear las intrusiones de manera activa. Los dos modos de operación usados por los sistemas de prevención de intrusos son la detección pasiva y la prevención en línea. En la detección pasiva, el IPS se encarga de interceptar el tráfico de la red, recibiendo una copia de todos los paquetes que circulan por ella. En caso de que detecte algún intruso, envía una alerta pero no puede frenar el ataque. Existe la posibilidad de que generen falsas alarmas y el mal funcionamiento de los dispositivos de la red puede hacer que cesen las alarmas. En la prevención en línea, el IPS está directamente en línea, envía alarmas y puede bloquear los ataques. La detección de errores y el mal funcionamiento pueden deberse a la interrupción del servicio (Piper, 2011).

4.1.6 LA PREVENCIÓN EN NUESTRO CONTEXTO

La prevención, para este trabajo de investigación, es el conjunto de estrategias dirigidas a evitar o reducir los daños causados por los incidentes de seguridad que pueden presentarse en un sistema de información mediante la definición de políticas, la concientización de los usuarios y la mitigación de vulnerabilidades y amenazas.

Este tipo de prevención se basará en un enfoque a largo plazo, en el que se tomarán medidas de seguridad enfocadas a evitar que ocurran los incidentes como: el establecimiento de políticas, el desarrollo de programas de concientización etc.; y en un enfoque a corto plazo, que buscará la reacción rápida ante los incidentes que se estén presentando, a fin de evitar daños mayores, analizando las causas e instaurando las medidas de seguridad necesarias para que no ocurran nuevamente.

4.2 EVOLUCIÓN DEL CONCEPTO DE RIESGO

El concepto de riesgo es complejo, causando una gran cantidad de ambigüedad entre los científicos. El significado del riesgo ha evolucionado con el tiempo y su desarrollo ha sido esbozado por desde el siglo XVII hasta la fecha. El concepto de riesgo se originó en el siglo XVII en las matemáticas relacionadas con los juegos de azar, en ellas el riesgo es una combinación entre la probabilidad y la magnitud de las pérdidas y las ganancias potenciales. Durante el siglo XVIII, el riesgo, visto como un concepto neutral, todavía era considerado como las ganancias y las pérdidas, y fue empleado en el negocio de los seguros marítimos. El riesgo en el estudio de la economía surgió en el siglo XIX. El concepto de riesgo, ahora, parecía más negativo, causando que los empresarios acudieran a incentivos especiales para que se tomara el riesgo que implicaba la inversión. En el siglo XX, una connotación totalmente negativa fue hecha al referirse al riesgo en la

ingeniería y la ciencia como los peligros que plantean los avances tecnológicos modernos, en la industria nuclear y petroquímica (Gerber & Von Solms, 2005).

Las definiciones de riesgo, en general, son descritas por la *Royal Society* empezando con "la probabilidad de que un evento adverso particular ocurra durante un período de tiempo establecido o resulte de un desafío particular"(Royal_Society, 1992). Para los ingenieros y científicos del grupo de estudio de la *Royal Society*, el reporte de 1992 incluye una definición de riesgo, basada en el estándar británico 4778, como "la combinación de la probabilidad o de la frecuencia de ocurrencia de un peligro definido y la magnitud de las consecuencias de su ocurrencia"(British_Standards_Institution, 1991)

Para una mejor comprensión del término riesgo y su relevancia a nivel científico, es necesario discutir las diversas ciencias con más detalle. Cuando se investiga la clasificación de las diferentes ciencias, se hace evidente que se pueden distinguir tres paradigmas, a saber: el paradigma de las ciencias naturales, el paradigma de las ciencias teóricas o abstractas y el paradigma de las ciencias sociales.

Las ciencias naturales son definidas en el diccionario Oxford como: "las ciencias que se usan en el estudio del mundo físico" (*Oxford Advanced Learner's Dictionary*, 1995), "que se ocupan de los objetos, fenómenos o leyes de la naturaleza y del mundo físico" . Cabe señalar que de acuerdo a (*Original Roget's Thesaurus of English Words and Phrases*, 1992) el término inglés *science,* es usualmente considerado un sinónimo de las ciencias naturales (Suojanen, 2000.).

El paradigma de las ciencias naturales agrupa varias disciplinas científicas, como las ciencias físicas, las ciencias de la vida y las ciencias aplicadas (*Original Roget's Thesaurus of English Words and Phrases*, 1992). Las ciencias de la vida incluyen aquellos temas relacionados con el estudio de las plantas, animales, etc., como la biología, la botánica; mientras que la ciencias físicas se ocupan del estudio de los objetos naturales inanimados o no vivos (*Oxford Advanced Learner's Dictionary*, 1995). Ejemplos de temas, que pueden clasificarse bajo las ciencias físicas, son la física, la química, la astronomía y la meteorología.

Las ciencias aplicadas se encargan de la aplicación práctica de los conocimientos de las ciencias puras, como la física o la química, a problemas prácticos (Infoplease.com). Un ejemplo de una ciencia aplicada es la ingeniería. La Ingeniería es la aplicación práctica de cualquiera de los principios científicos o matemáticos derivados del conocimiento de las ciencias matemáticas y naturales (Stark, 2003), para cumplir con fines prácticos en la industria o el comercio. La Ingeniería eléctrica no es más que uno de los diferentes campos en los que se divide la ingeniería. Como se muestra en la Figura 3. La ingeniería informática se considera una de las ramas de la ingeniería eléctrica (Stark, 2003).

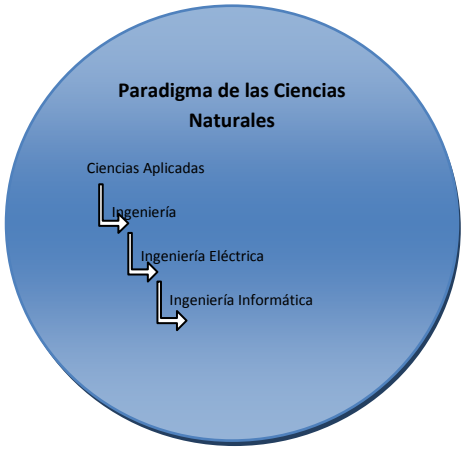

Figura 3: Jerarquía en el paradigma de las ciencias naturales
Fuente: *Management of Risk in the Information Age* (Gerber & Von Solms, 2005)

La ingeniería informática, casi desconocida hace tan sólo unas décadas, ahora se clasifica como uno de los campos de más rápido crecimiento. La micro-miniaturización es una de las tendencias actuales de la ingeniería informática. Otra tendencia es el uso de procesadores paralelos y materiales superconductores(Stark, 2003) para aumentar la velocidad de computo. Sin embargo, la creación de programas sofisticados para promover la "inteligencia artificial" y el desarrollo de los lenguajes de máquina de alto nivel se considera que están más cercanos a las ciencias de la computación que a la ingeniería informática (Weems, 2003).

Las ciencias de la computación son una combinación entre teoría, ingeniería y experimentación. Estas proveen una plataforma para el diseño y uso de los computadores. Basados en el conocimiento que, las ciencias de la computación se originaron a partir de las matemáticas e ingeniería (Weems, 2003), se cree que las ciencias de la computación están posicionadas en un terreno común entre el paradigma de las ciencias naturales y el paradigma de las ciencias teóricas (abstractas) como se muestra en la Figura 4. Por consiguiente, sus enfoques son considerados como altamente matemáticos y lógicos. No fue hasta la introducción de los primeros computadores en 1940 que la ciencias de la computación fueron reconocidas como diferentes de las matemáticas y la ingeniería (Weems, 2003). A pesar de sus diferencias, los campos de las ciencias de la computación y la ingeniería informática (una rama de la ingeniería) están estrechamente relacionados (Stark, 2003) dentro del paradigma de las ciencias naturales, como se muestra en la Figura 4.

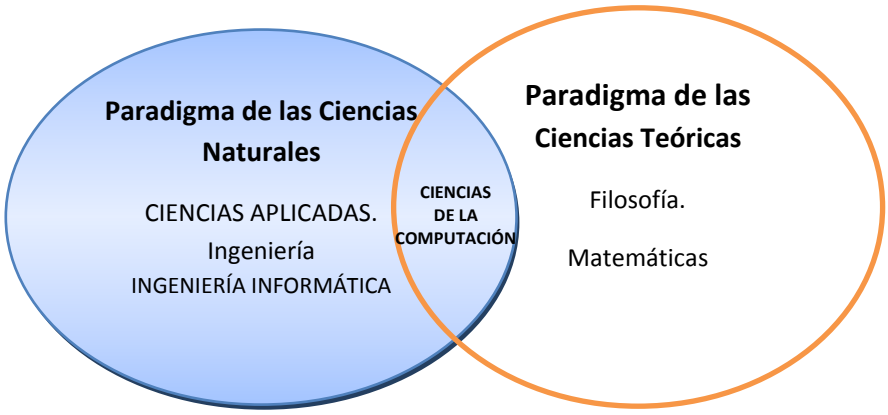

Figura 4: Posición de las ciencias de la computación dentro del paradigma de las ciencias naturales y el paradigma de las ciencias teóricas
Fuente: *Management of Risk in the Information Age* (Gerber & Von Solms, 2005)

La ciencias naturales o ciencias, como se les denomina alternativamente, se desarrollan utilizando un enfoque sistemático, conocido como método científico, basado en un análisis objetivo en lugar de creencias personales (Burnie, 2003). Esta característica de las ciencias naturales, distingue a las ciencias naturales de las ciencias sociales.

Dentro del paradigma de las ciencias sociales, las ciencias sociales se definen como el estudio de la sociedad y el comportamiento social, o una ciencia o campo de estudio que trata de un aspecto de la sociedad o de las formas de actividad social (Infoplease.com) (*Oxford Advanced Learner's Dictionary*, 1995). El *U.S Department of Labor* (U.S._Department_of_Labor, 2003) especifica que se trata de un estudio que involucra a todos los aspectos de la sociedad - cubriendo eventos pasados y logros, así como el comportamiento humano y las relaciones entre los grupos. Las ciencias sociales incluyen disciplinas como la economía, la política, el gobierno, la legislación, el derecho, la justicia penal, la antropología, la cultura, la ética, la religión, la historia, la geografía, la psicología, la sociología y gerontología (University_of_Maryland, 2003) (Central_Oregon_Community_College, 2003) (Miami-Dade_Community_College, 2003) (U.S._Department_of_Labor, 2003) (Glenn, 2001). Se puede argumentar que la diferencia más obvia entre las ciencias naturales y las ciencias sociales es que, las ciencias naturales se ocupan más de los fenómenos objetivamente medibles, mientras que las ciencias sociales están más involucradas con la conducta humana y la actividad social.

La pregunta que surge ahora es ''¿cómo el concepto de riesgo y la evaluación del mismo se relacionan con los dos paradigmas definidos? El concepto de riesgo en el paradigma de las ciencias naturales es visto como un riesgo objetivo o evaluado, debido a los métodos científicos de valoración utilizados para evaluar el riesgo. Una evaluación objetiva del riesgo no se basa en juicios (Kirkwood, 1994) y sigue cálculos precisos, fórmulas y experimentos exactos. Dentro del paradigma de las ciencias sociales, sin embargo, el riesgo se considera como riesgo subjetivo o percibido, ya que es una decisión a la que se llegó sin una evaluación científica. La evaluación subjetiva del riesgo se basa en la percepción, la heurística o la regla-de-oro de las directrices. Siendo la regla de oro una decisión a la que se llega mediante la utilización de experiencia, juicio e ingenio (Kirkwood, 1994) en lugar de las matemáticas puras. De esto se puede ver que hay una clara diferencia en la forma en que se evalúan los riesgos en el paradigma de las ciencias naturales frente al paradigma de las ciencias sociales.

En las tecnologías de la información parece apropiado considerar la definición de riesgo que dió NIST (*National Institute of Standards and Technology*) en 1995: “es la posibilidad de que ocurra algo adverso” (NIST, 1995). Luego, en el 2001, NIST redefinió el riesgo como: “el impacto negativo neto debido a una vulnerabilidad, considerando su probabilidad y el impacto de ocurrencia” (NIST, 2001). Otra definición de riesgo, relacionada con el ambiente computacional, fue establecida por Kailay y Jarratt (Kailay & Jarratt, 1995), “es el potencial del daño a un sistema, o a los activos asociados, que existe como resultado de la combinación de una amenaza de seguridad y una vulnerabilidad”. Por tanto, existe el riesgo debido a la combinación de amenazas, vulnerabilidad y valor de los activos.

Una vulnerabilidad es una debilidad en el sistema de seguridad que puede ser explotada para causar la pérdida o el daño al activo (Pfleeger, 1989) y una amenaza es la fuente o circunstancia que tiene el potencial para causar pérdida o daño (Kailay & Jarratt, 1995) (Pfleeger, 1989) (Gerber & Von Solms, 2005).

4.2.1 EL RIESGO EN NUESTRO CONTEXTO

El riesgo, para este trabajo de investigación, es la probabilidad de que un evento adverso ocurra y afecte a un sistema de información y a sus activos asociados (personas, información, infraestructura) como resultado de la combinación de una amenaza de seguridad y una vulnerabilidad, causando pérdidas o daños a la organización.

La valoración del riesgo no va a consistir en identificar solamente las fallas técnicas sino también en identificar cuestiones sociales como la percepción del riesgo, el sesgo cultural, la falta de concientización y las fallas en la comunicación humana, dando como resultado un riesgo objetivo o evaluado basado en métodos científicos y un riesgo subjetivo o percibido basado en la experiencia y el juicio.

4.3 GESTIÓN DEL RIESGO

El término “gestión” es objeto de debates en algunos círculos académicos que intentan desentrañar su esencia epistemológica y lo comparan, en varias ocasiones, con el de “administración”. Ambos tienen un denominador común cuando se relacionan con la operación de procesos, dirección y control. El uso más difundido de gestión se asocia a la traducción de su palabra similar en inglés: *management*. Juan Casassus (Casassus, 2000) la entiende como “la capacidad de articular los recursos de que se dispone de manera de lograr lo que se desea” .

La gestión del riesgo se utiliza en muchas áreas (seguridad de la información, finanzas, seguros..). En el ámbito de la privacidad, los únicos riesgos a tener en cuenta son los que el tratamiento de datos personales plantea a la privacidad. Esos riesgos están compuestos por un evento temido (¿a qué tenemos miedo?) y todas las amenazas que hacen que sea posible (¿cómo puede ocurrir esto?) (CNIL, 2012).

El *Australian/New Zealand Standard* considera la gestión del riesgo como: “Un proceso iterativo conformado por pasos bien definidos que llevados a cabo de manera secuencial, constituye el fundamento para la adecuada toma de decisiones, al proporcionar un mejor conocimiento de los riesgos y del impacto de los mismos.”. Mientras que la administración de riesgos se refiere al “proceso general por el que se analizan y gestionan los riesgos” (Gerber & Von Solms, 2005).

Dickson (Dickson, 1995) señala que: “la gestión del riesgo es un mecanismo para gestionar la exposición al riesgo que nos permite reconocer los sucesos que pueden desembocar en consecuencias desafortunadas o dañosas en el futuro, su gravedad y cómo pueden ser controlados”. Añade también una definición práctica: “la identificación, analisis y control económico de aquellos riesgos que pueden amenazar los resultados o la capacidad de ganancia de una empresa.”

Aunque la ingeniería se centra más en la tecnología que en las personas (Frosdick, 1997), los ingenieros saben que ''la percepción del riesgo depende en gran medida de las creencias, sentimientos y juicios, y tiene gran influencia sobre la tolerancia o aceptación del riesgo'' (Strutt, 1993). Sin embargo, las técnicas utilizadas en la ingeniería, que forma parte del paradigma de las ciencias naturales, se preocupan más por la identificación de las fallas técnicas que de cuestiones sociales, como la percepción del riesgo, el sesgo cultural y fallas en la comunicación humana.

Los científicos sociales se oponen fuertemente a esta visión de los científicos naturales y los ingenieros en cuanto a la gestión de riesgos y advierten que hacer caso omiso de las cuestiones sociológicas/sociales podría resultar problemático, ya que el resultado de un error humano o falta de comunicación puede ser tan desastroso como el resultado de una falla técnica (Frosdick, 1997).

Las técnicas de evaluación del análisis de riesgos deben consecuentemente tratar el riesgo como una construcción colectiva, porque cuando se trata de lo que es un riesgo aceptable, existen diferentes juicios (Frosdick, 1997). El juicio varía de la percepción subjetiva a la ciencia física, y en el centro hay un área de creencias y valores compartidos (Douglas & Wildavsky, 1982). El Dr. Michael Hartoonian del Departamento de Educación y Desarrollo Temprano de Alaska afirma que separar las herramientas de la cultura conduce a verdades a medias y a la desilusión .

La aplicación de estos puntos de vista a la gestión global del riesgo muestra que el análisis de riesgos no sólo debe considerar los procesos científicos del paradigma de las ciencias naturales. Se recomienda que, a pesar de contribuir a la subjetividad, los elementos del paradigma de las ciencias sociales deben tenerse en cuenta. Deuchar (Deuchar, 2003), director general de la empresa de contratación, *The Oval Office*, dice que el componente de riesgo humano podría costar millones en indemnizaciones por despido, entrenamiento y tasas de colocación, pérdida de productividad, daños indirectos a la imagen de la compañía y pérdida de oportunidades, todo porque el factor humano a menudo se deja fuera de la ecuación de gestión de riesgos. Por lo tanto, cuando se trata de visualizar la gestión de riesgos en el contexto de los dos paradigmas definidos, se hace evidente que el paradigma de las ciencias naturales y el paradigma de las ciencias sociales deben unirse, provocando una superposición donde la información es el punto de conexión. Esta afirmación está respaldada por Roth (Roth, 2003), jefe del equipo de Servicios Legales de Riesgo Alexander Forbes, quien afirma “la información, en todas sus formas, es sin duda uno de los activos más importantes de una organización. En este contexto, la "información"

se refiere a algo más que tecnología. Se refiere a la integridad, disponibilidad y confidencialidad del alma de la organización, incluidos los secretos empresariales del negocio, relaciones contractuales, sistemas financieros y operacionales, detalles de clientes y transacciones e información anunciada al público". Esto muestra claramente que el paradigma de las ciencias naturales y el paradigma de las ciencias sociales están incluidos cuando se hace referencia a la información (Gerber & Von Solms, 2005).

4.3.1 ANÁLISIS DE RIESGOS

La gestión de riesgos debe ir precedida de una actividad de análisis de riesgos (Bandyopadhyay, Mykytyn, & Mykytyn, 1999) (Owens, 1998) (BS7799-2, 1999) (Moses, 1992). En conjunto, el proceso de análisis de riesgos seguido por el proceso de gestión de riesgos puede considerarse como parte de la administración global del riesgo.

Frosdick (Frosdick, 1997) define el análisis de riesgos como la suma de identificación, estimación y evaluación del riesgo (ver Figura 5).

El escenario básico del análisis de riesgos, como se ilustra en la Figura 5, es la identificación de riesgos (Tchankova, 2002). Como su nombre lo indica, su propósito principal es el de identificar los riesgos y el riesgo comprende una combinación de activos, amenazas y vulnerabilidad (ISO/IEC_TR_13335-1, 1996). Por tanto, es necesario identificar los activos de TI (dentro de un límite establecido), identificar las amenazas de los activos y tener en cuenta las vulnerabilidades (Jung, Han, & Suh, 1999).

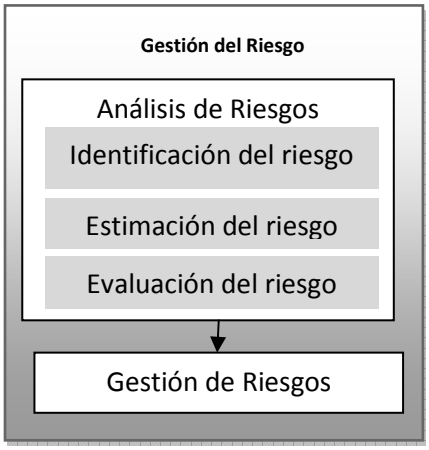

Figura 5: Procesos dentro de la gestión global del riesgo
Fuente: *Management of Risk in the Information Age* (Gerber & Von Solms, 2005)

Una vez que los riesgos han sido identificados, sigue la estimación del riesgo. La estimación del riesgo no es más que colocar valores al riesgo. Los valores monetarios que se asignan, preferentemente, deben estar relacionados con el costo de obtener y mantener el activo (Humphreys, Moses, & Plate, 1998). Los riesgos identificados se suelen cuantificar de acuerdo a un enfoque de dos dimensiones: teniendo en cuenta la probabilidad de ocurrencia del riesgo y sus consecuencias en caso de que ocurra. Los árboles de fallos y de eventos pueden ayudar en el cálculo de la probabilidad de diversos eventos que se producen, mientras que la cuantificación de

las consecuencias se puede lograr mediante el uso de una combinación de las técnicas de modelado computacional, y pruebas o juicios de valor de expertos (Frosdick, 1997).

Una vez que los riesgos se han cuantificado, por estimar tanto su probabilidad de ocurrencia como la magnitud de sus consecuencias, pueden ser evaluados para indicar la tolerancia o aceptabilidad de los mismos. De ahí que el término evaluación de riesgos se confunda a menudo con el análisis de riesgos pero es, de hecho, la tercera etapa del análisis de riesgos. La evaluación de riesgos no es más que el cálculo del riesgo basado en los valores asignados durante la estimación del riesgo, a la probabilidad y magnitud (impacto o gravedad del daño).

El proceso de evaluación de riesgos se refiere a menudo como ""evaluación de riesgos probabilística '' que es un proceso de tres etapas. En primer lugar, determinar lo que puede salir mal; en segundo lugar, determinar la probabilidad de que salga mal; y en tercer lugar, determinar la gravedad de las consecuencias que tendría si sale mal. (Kirkwood, 1994) define el valor del riesgo como se muestra en la ecuación (1).

Riesgo= Probabilidad x Gravedad del daño (1)

La evaluación de riesgos, de esta manera, coloca una connotación negativa en el riesgo y señala que el riesgo es malo. Sin embargo, el riesgo sigue siendo un concepto neutral. Una versión más refinada de Kirkwood del riesgo como un concepto neutral es la mostrada en la ecuación (2).

Riesgo=Probabilidad x (Efectos dañinos - Efectos benéficos) (2)

La estimación del riesgo, incluyendo su probabilidad de ocurrencia y severidad del daño, requiere un conocimiento profundo, experiencia y dominio del tema (Jung et al., 1999). Incluso con la disponibilidad de los analistas de riesgos con experiencia, el análisis de riesgo a menudo se basa nada más en meras conjeturas (Pfleeger, 1997). Dar una respuesta involucra técnicas cuantitativas y cualitativas de análisis de riesgos, y estas han contribuido en gran medida a la naturaleza subjetiva del análisis de riesgos, como lo han señalado y comentado muchos investigadores (Bandyopadhyay et al., 1999) (Fung, Kwok, & Longley, 2003) (Pfleeger, 1997) (Lichtenstein, 1996) (Kirkwood, 1994) (Jacobson, 1996). De acuerdo con Kirkword (Kirkwood, 1994), el riesgo que aparece como el resultado de una evaluación científica se conoce como riesgo objetivo o evaluado, mientras que una decisión sobre la existencia del riesgo sin una evaluación científica, se conoce como riesgo subjetivo o percibido.

Debido que el análisis de riesgos asegura que los procesos de toma de decisiones en la gestión de riesgos sean científicamente informados y ya que esto va de la mano con la identificación y evaluación de los riesgos para proteger, principalmente, activos físicos (tangibles), por ejemplo, la infraestructura y el hardware, se asume que este encaja dentro del paradigma de la ciencias naturales (Gerber & Von Solms, 2005).

4.3.2 GESTIÓN DE RIESGOS

Una vez el proceso de análisis de riesgos está completo, debe seguir la gestión de riesgos. La gestión de riesgos se refiere a “las actividades de planeación, monitorización y control que se

basan en la información producida en el análisis de riesgos"(Scarff, Carty, & Charette, 1993). Se trata de la identificación e implementación de controles de seguridad para reducir los riesgos a un nivel aceptable, según lo indicado por la evaluación de riesgos (Moses, 1992). La reducción del riesgo se puede lograr evitando el riesgo, transfiriendo el riesgo, reduciendo la probabilidad de las amenazas, reduciendo las vulnerabilidades, reduciendo los posibles impactos, detectando tempranamente eventos no deseados, o reaccionando y recuperándose de algún incidente (Moses, 1992). La alternativa que se tome para reducir el riesgo depende del entorno empresarial específico y las circunstancias en las que la organización lleva a cabo su negocio. Incluso después de implementar todos los controles de seguridad, todavía existirá algún tipo de riesgo. El riesgo restante se denomina riesgo residual. Este riesgo podría ser el resultado de algunos activos dejados intencionalmente sin protección, ya sea a causa del bajo riesgo que representan o debido al alto costo del control sugerido. El riesgo residual debe ser clasificado como "aceptable" o "inaceptable". El riesgo inaceptable no debe tolerarse y las decisiones deben ser tomadas para aplicar controles adicionales o controles más estrictos, lo que reducirá aún más el riesgo (Humphreys et al., 1998).

Debe tenerse en cuenta que la gestión de riesgos, sin embargo, no termina cuando la gestión del riesgo se ha completado. Es un proceso continuo que depende directamente de los cambios del entorno interno y externo de la organización (Tchankova, 2002). Es un hecho que el cambio es inevitable. Sobre todo en el entorno de TI, donde los rápidos avances de la tecnología se llevan a cabo y se espera que continúe avanzando a un ritmo acelerado en el futuro (Gerber & Von Solms, 2005).

4.3.3 PREVENCIÓN DE RIESGOS EN NUESTRO CONTEXTO

La prevención de riesgos, para este trabajo de investigación, es un proceso continuo que consiste en analizar los riesgos existentes en un sistema de información, planear y ejecutar actividades, a corto y largo plazo, tendientes a evitar o reducir esos riesgos identificados, evaluar la efectividad de dichas actividades y actualizarlas, de acuerdo a los cambios en el entorno interno y externo de la organización.

4.4 GESTIÓN DE LA INFORMACIÓN

Existen muchos términos relacionados con la gestión, como: gestión ambiental, gestión social, gestión educativa y gestión cultural. Cuando se trata del manejo de la información y el conocimiento, se hace referencia a los conceptos de gestión de información y gestión del conocimiento. Ambos términos están indisolublemente ligados, debido a que uno antecede al otro como un proceso continuo. No puede existir gestión del conocimiento sin una gestión de información previa y exitosa .

Según Ponjuán (Ponjuan Dante, 2004), la gestión de información es "un proceso mediante el cual se obtienen, despliegan o utilizan recursos básicos para manejar información dentro y para la sociedad a la que sirve". Tiene como elemento básico la gestión del ciclo de vida de este recurso y se desarrolla en cualquier organización. La GI (Gestión de la Información), debido al impetuoso desarrollo de las TIC, sucede cada vez más en entornos virtuales, como portales y plataformas

Web, y hace uso de herramientas informáticas cada vez más sofisticadas y, al mismo tiempo, más amigables y accesibles, por lo que los propios usuarios se convierten a menudo en gestores de información. .

Por otra parte, Carlota Bustelo y Raquel Amarilla (Bustelo Ruesta & Amarilla Iglesias, 2001) definen la gestión de la información como: “el conjunto de actividades realizadas con el fin de controlar, almacenar y, posteriormente, recuperar adecuadamente la información producida, recibida o retenida por cualquier organización en el desarrollo de sus actividades."

La gestión de información personal (PIM – *Personal Information Management*) es definida por Lansdale (Lansdale, 1988) como “los métodos y procedimientos mediante los cuales manejamos, categorizamos y recuperamos información en el día a día”. Barreau (Barreau, 1995) la describe como un “sistema desarrollado por un individuo para uso personal, en un entorno laboral”; tal sistema incluye “los métodos y las reglas de la persona para obtener la información [...], los mecanismos para organizarla y almacenarla, las reglas y los procedimientos para mantener el sistema, los mecanismos de recuperación, y los procedimientos para producir resultados”.

Boardman (Boardman, 2004) señala que “muchas definiciones de la PIM derivan de una perspectiva tradicional, según la cual la información se almacena para que pueda ser recuperada en el futuro”. Y Jones (Jones, 2007), apunta que la PIM es “la práctica y el estudio de las acciones que un individuo ejecuta para obtener o crear, almacenar, organizar, mantener, recuperar, utilizar y distribuir la información necesaria para completar tareas (relacionadas o no con el trabajo) y cumplir con diversos roles y responsabilidades (familiares, laborales, sociales, comunitarios)”.

La investigación sobre la PIM se ocupa de resolver una cuestión: garantizar que una fuente o un canal de información, una vez localizado, volverá a estar disponible cuando quiera que se necesite. La información es un recurso valioso, aunque su valor no es intrínseco a ella misma. Y porque además es un recurso muy abundante, es necesario organizarla y gestionarla, porque gestionar la información es la manera más tangible de gestionar otros recursos (tiempo, dinero, bienestar, conocimiento), que sí son intrínsecamente valiosos (Franganillo, 2009).

4.4.1 MANEJO DE LA INFORMACIÓN PERSONAL EN NUESTRO CONTEXTO

En nuestra investigación, el manejo de la información personal se define como el conjunto de actividades realizadas para almacenar, organizar, obtener, modificar, recuperar, utilizar, distribuir y proteger la información necesaria para completar las diversas tareas que realizan los usuarios de un sistema de información y cumplir así con sus roles y responsabilidades.

El manejo adecuado de la información personal es una parte importante de la gestión de la información, pues si se toman las medidas de seguridad necesarias para que esta información no caiga en manos indeseadas, los sistemas de información también estarán protegidos, lo que evitará fraudes,extorsiones, suplantaciones, etc.

4.5 METODOLOGÍAS DE PREVENCIÓN DE RIESGOS

Independientemente de la gran cantidad de definiciones, en este trabajo se considerará que una Metodología de Prevencion de Riesgos es un conjunto de pasos que se llevan a cabo anticipadamente para mitigar la proximidad de un daño y asi evitar el mal tratamiento de los datos personales que puede colocar en riesgo la seguridad de una entidad o institución.

En la literatura, no se encontraron muchas metodologías que se centren exclusivamente en la prevención de riesgos, sino que la prevención hace parte de la gestión de riesgos, por eso se describen dichas metodologías.

4.5.1 METODOLOGÍAS DE ANÁLISIS Y GESTIÓN DE RIESGOS

4.5.1.1 OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

OCTAVE es una metodología de análisis de riesgos desarrollada por la Universidad Carnegie Mellon en el año 2001, y su acrónimo significa "*Operationally Critical Threat, Asset and Vulnerability Evaluation*". OCTAVE estudia los riesgos en base a tres principios: confidencialidad, integridad y disponibilidad. Esta metodología es utilizada por distintas agencias gubernamentales tales como el Departamento de Defensa de Estados Unidos (DoD) (SecurityArtWork). En la Figura 6 se muestran las fases llevadas a cabo en esta metodología.

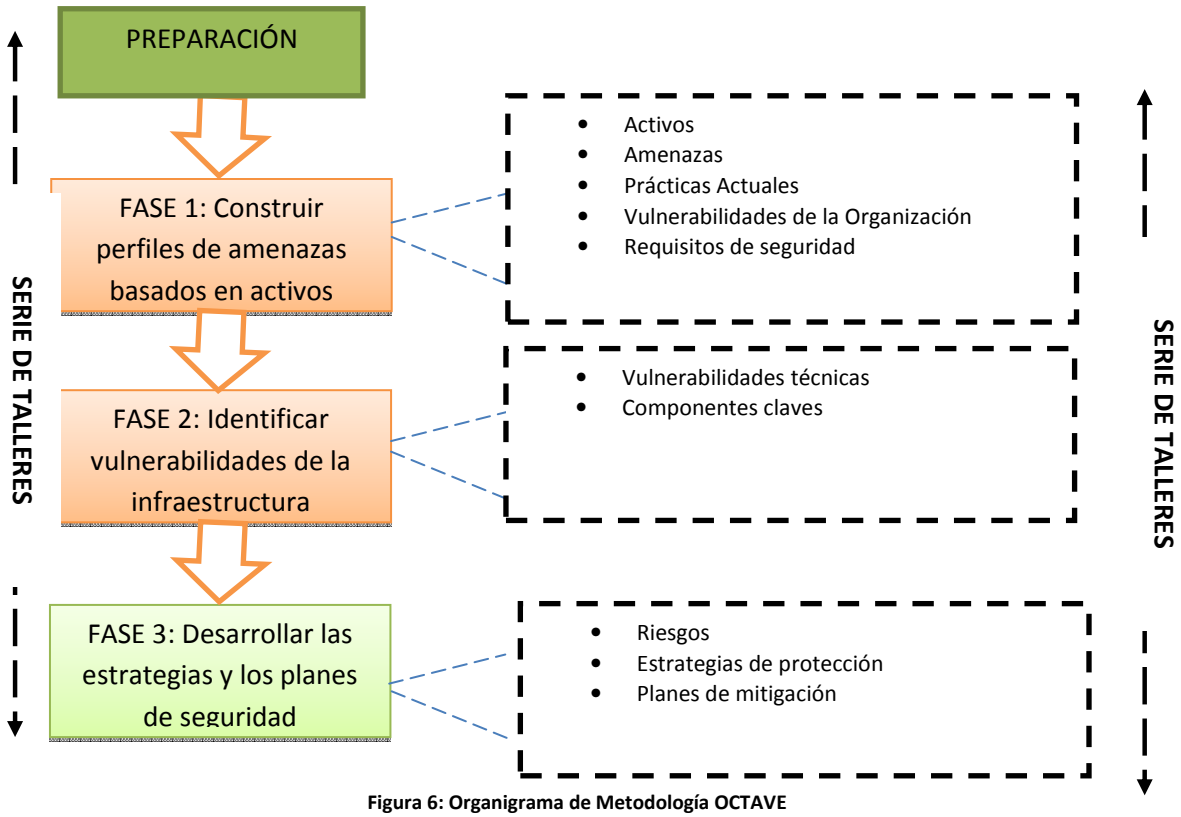

Figura 6: Organigrama de Metodología OCTAVE

Fuente: Autor, basada en Introducción al Análisis de Riesgos – Metodologías (II) (SecurityArtWork)

Las tres fases de esta metodología se definen así (Alberts & Dorofee, 2001):

- **Fase 1- Construir Perfiles de Amenazas Basados en Activos:** Esta es una evaluación organizacional. Se examinan las áreas clave de experiencia dentro de la organización para identificar los activos de información importantes, las amenazas a los activos, los requisitos de seguridad de los activos, lo que la organización está haciendo para proteger sus activos de información (estrategias prácticas de protección), y debilidades en las políticas organizacionales y prácticas (vulnerabilidades organizacionales). Los procesos que se llevan a cabo en esta fase son:

    - Proceso 1: Identificar el conocimiento de la alta gerencia.
    - Proceso 2: Identificar el conocimiento del área operacional.
    - Proceso 3: Identificar el conocimiento del personal.
    - Proceso 4: Crear perfiles de amenazas.

- **Fase 2- Identificar Vulnerabilidades de la Infraestructura:** Se trata de una evaluación de la estructura de la información. Los componentes operativos clave de las tecnologías de información se examinan en busca vulnerabilidades tecnológicas que pueden conducir a una acción no autorizada. Los procesos que se llevan a cabo en esta fase son:

    - Proceso 5: Identificar los componentes clave.
    - Proceso 6: Evaluar los componentes seleccionados.

- **Fase 3 -Desarrollar las Estrategias y los Planes de Seguridad:** Los riesgos se analizan en esta fase. La información generada por las evaluaciones de la infraestructura organizativa y de la información (Fases 1 y 2) se analizan para identificar riesgos para la empresa y para evaluar los riesgos en función de su impacto en la misión de la organización. Además, se desarrolla una estrategia de protección para los planes de organización y de mitigación que aborden los riesgos de más alta prioridad. Es en esta fase donde se implementaría la prevención de riesgos dentro de la estrategia de protección. Los procesos que se llevan a cabo en esta fase son:

    - Proceso 7: Análisis de riesgos de conducta.
    - Proceso 8: Fomentar la estrategia de protección.

4.5.1.2 CORAS

CORAS es un proyecto de investigación y desarrollo tecnológico europeo, que está elaborando una herramienta soportada en un marco para la evaluación de riesgos de seguridad basado en modelos. CORAS proporciona un lenguaje personalizado para el modelado de amenazas y riesgos, y viene con directrices detalladas que explican cómo el lenguaje que se debe utilizar para capturar y modelar la información pertinente durante las diversas etapas del análisis de la seguridad (Norsk_Regnesentral, 2000). El Lenguaje Unificado de Modelado (UML) se suele utilizar para modelar el objeto del análisis. Para documentar los resultados intermedios y para la presentación de las conclusiones generales, se usan diagramas especiales CORAS que se inspiran en UML. El método CORAS proporciona una herramienta informática diseñada para soportar la

documentación, mantenimiento y los reportes del análisis de resultados a través de modelos de riesgo. En el método CORAS, un análisis de riesgos de seguridad se lleva a cabo en siete pasos (ver Figura 7) (Norsk_Regnesentral, 2000).

Figura 7: Pasos de Método CORAS.

- **Paso 1**: El primer paso consiste en una reunión introductoria. El principal punto de la agenda de esta reunión es conseguir que los representantes del cliente presenten sus objetivos generales del análisis y lo que desean analizar. Por lo tanto, durante la etapa inicial los analistas reunirán la información basada en las presentaciones y discusiones del cliente.

- **Paso 2:** El segundo paso implica otra reunión con los representantes del cliente. Sin embargo, esta vez los analistas presentarán su comprensión de lo que entendieron en la primera reunión y del estudio de la documentación que puso a su disposición el cliente. El segundo paso implica también un análisis básico de la seguridad de alto nivel. Durante este análisis se identifican las primeras amenazas, vulnerabilidades, escenarios de amenaza e incidentes no deseados. Ellos serán utilizados para ayudar con la dirección y la determinación del alcance del análisis más detallado aún por realizarse.

- **Paso 3:** El tercer paso consiste en una descripción más precisa del objeto a analizar, y también de todos los supuestos y otras condiciones previas hechas. El tercer paso se termina una vez que toda esta documentación ha sido aprobada por el cliente.

- **Paso 4:** Este paso se organiza como un taller, proveniente de personas con experiencia en el objeto del análisis. El objetivo es identificar el mayor número de posibles incidentes no deseados como sea posible, así como las amenazas, vulnerabilidades y escenarios de amenaza.

- **Paso 5:** En el quinto paso también se organiza un taller, esta vez enfocado en la estimación de las consecuencias y los valores de probabilidad para cada uno de los incidentes no deseados identificados.

- **Paso 6:** Este paso le da al cliente el primer cuadro de riesgo general. Normalmente, esto dará lugar a algunos ajustes y correcciones.

- **Paso 7:** El último paso se dedica a la identificación del tratamiento, así como abordar cuestiones de costo/beneficio de los tratamientos. En este tratamiento de los riesgos es donde se introduciría la prevención de riesgos. Esta etapa se organiza mejor como un taller.

4.5.1.3 Metodología de Administración de Riesgos según Estándar Australiano

La administración de riesgos es una parte integral del proceso de administración, la cual es multifacética e iterativa y de mejora continua. Esta se desarrolla en 5 fases, las cuales son (*AS/NZS 4360:1999 -Estándar Australiano, Administración de Riesgos*, 1999) (ver Figura 8):

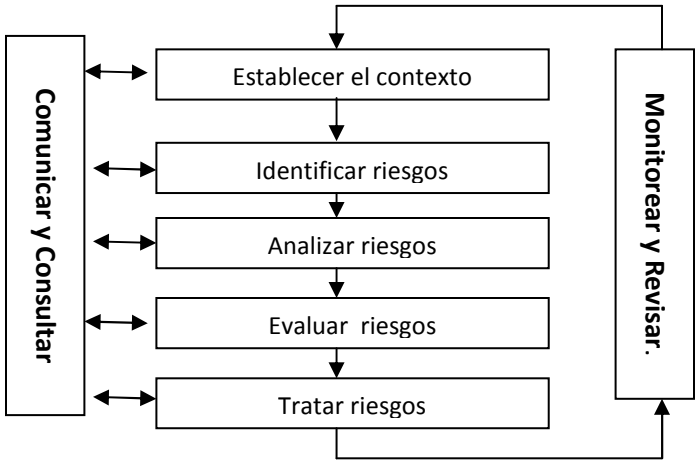

Figura 8 Vista general de la Administración de Riesgos
Fuente: Estándar Australiano Administración de Riesgos (*AS/NZS 4360:1999 -Estándar Australiano, Administración de Riesgos*, 1999)

- **Establecer el Contexto:** Dentro de esta fase se definen los parámetros básicos del proceso que ocurre dentro de la estructura organizacional de acuerdo al contexto estratégico, organizacional, y de administración de riesgos. Esto da como resultado el desarrollo de criterios de evaluación y una guía para la toma de decisiones.

- **Identificar Riesgos:** Este paso busca identificar los riesgos a administrar. Es crítica una identificación amplia utilizando un proceso sistemático bien estructurado, porque los riesgos potenciales que no se identifican en esta etapa son excluidos de un análisis posterior. La identificación debería incluir todos los riesgos, estén o no bajo control de la organización. La finalidad de esta segunda etapa es generar una lista amplia de eventos de los cuales es necesario considerar causas y escenarios posibles para luego utilizar herramientas como: listas de chequeo, juicios basados en experiencias, registros en diagramas de flujo, análisis de sistemas y análisis de escenarios.

- **Analizar Riesgos:** La finalidad de esta fase es separar los riesgos menores de los riesgos mayores y así proveer datos para la evaluación y tratamiento de los riesgos. Esta fase involucra prestar atención a las fuentes de riesgos, sus consecuencias y las probabilidades de que puedan ocurrir esas consecuencias. Se analiza el riesgo combinando estimaciones de consecuencias y probabilidades en el contexto de las medidas de control existentes. Se puede llevar a cabo un análisis preliminar para excluir del estudio detallado los riesgos similares o de bajo impacto. De ser posible los riesgos excluidos deberían listarse para demostrar que se

realizó un análisis de riesgos completo. Dentro de este proceso de análisis se siguen unos subprocesos como son: determinar los controles existentes, consecuencias y probabilidades, tipos de análisis.

- **Evaluar Riesgos:** Esta etapa involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente. La evaluación cualitativa involucra la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y la evaluación cuantitativa involucra la comparación de un nivel numérico de riesgo contra criterios que pueden ser expresados como un número específico, tal como, un valor de fatalidad, frecuencia o monetario. El resultado de una evaluación de riesgos es una lista de riesgos con prioridades para una acción posterior, basadas en los objetivos de la organización y el grado de oportunidad que podría resultar al tomar el riesgo. Los riesgos resultantes que caen dentro de las categorías de riesgos bajos o aceptables, pueden ser aceptados con un tratamiento futuro mínimo. Los riesgos bajos y aceptados deberían ser monitoreados y revisados periódicamente para asegurar que se mantienen aceptables.

- **Tratar los riesgos:** Este proceso involucra identificar el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos. Es aquí en esta etapa que tiene lugar la prevención. En la Figura 9 podemos identificar el proceso de tratamiento de riesgos.

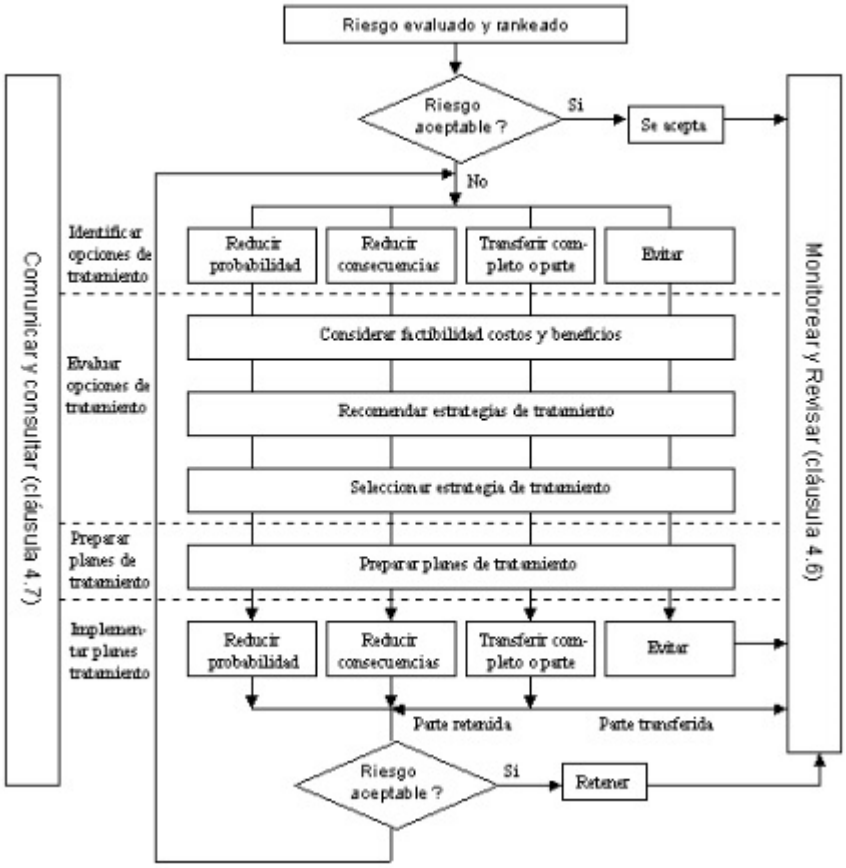

Figura 9. Proceso de Tratamiento de Riesgos
Fuente: Estándar Australiano Administración de Riesgos (*AS/NZS 4360:1999 -Estándar Australiano, Administración de Riesgos*, 1999)

4.5.1.4 NTC-ISO/IEC 27005: Gestión del Riesgo en la Seguridad de la Información

La gestión del riesgo en la seguridad de la información es una parte integral para todas las actividades de gestión de seguridad de la información y se aplica tanto a la implementación como al funcionamiento continuo de un SGSI (Sistema de Gestión de Seguridad de la Información).

El proceso de gestión del riesgo en la seguridad de la información consta del establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo y monitoreo y revisión del riesgo (ver Figura 10).

El enfoque iterativo suministra un buen equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, incluso garantizando que los riesgos altos se valoren de manera correcta.

Como lo muestra la Figura 10, el contexto se establece primero. Luego se realiza una valoración del riesgo. Si ésta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos hasta un nivel aceptable, entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo

otra iteración de la valoración del riesgo con un contexto revisado (por ejemplo, los criterios de evaluación del riesgo, los criterios para aceptar el riesgo o los criterios de impacto), posiblemente en partes limitadas del alcance total (ICONTEC, 2009).

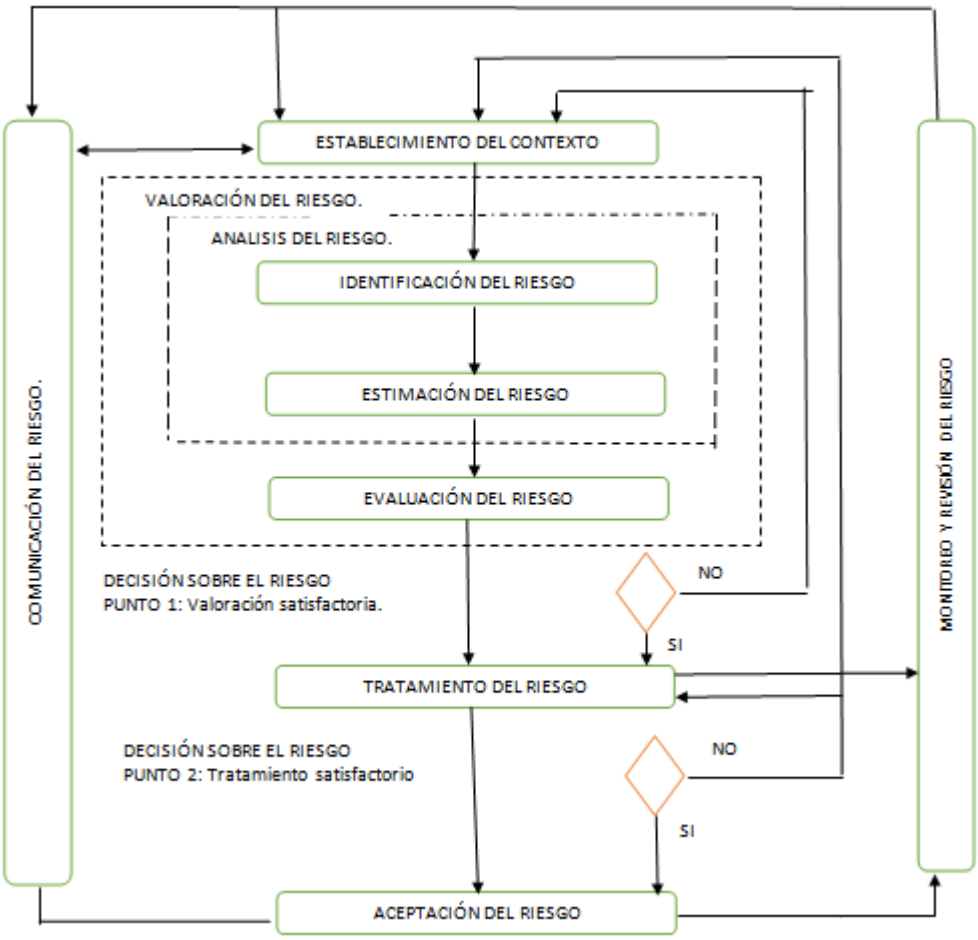

Figura 10. Proceso de gestión del riesgo en la seguridad de la información
Fuente: NTC-ISO/IEC 27005 (ICONTEC, 2009)

La eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual. En esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto (por ejemplo, criterios para valoración del riesgo, de aceptación o de impacto del riesgo), seguida del tratamiento del riesgo.

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la organización.

En un SGSI, el establecimiento del contexto, la valoración del riesgo, el desarrollo del plan de tratamiento del riesgo y la aceptación del riesgo son parte de la fase de “planificar”. En la fase de “hacer” del SGSI, se implementan las acciones y los controles que son necesarios para reducir el

riesgo hasta un nivel aceptable, de acuerdo con el plan de tratamiento del riesgo. En la fase de "verificar" del SGSI, los directores determinarán la necesidad de revisiones de las valoraciones y del tratamiento del riesgo a la luz de los incidentes y los cambios en las circunstancias. En la fase de "actuar", se llevan a cabo todas las acciones que son necesarias, incluyendo la aplicación adicional del proceso de gestión del riesgo en la seguridad de la información (ver Tabla 3) (ICONTEC, 2009).

Tabla 3. Alineamiento del SGSI y el proceso de gestión del riesgo de seguridad de la información
Fuente: NTC-ISO/IEC 27005 (ICONTEC, 2009)

Proceso de SGSI	Proceso de gestión del riesgo en la seguridad de la información
Planificar	Establecer el contexto Valoración del riesgo Planificación del tratamiento del riesgo Aceptación del riesgo
Hacer	Implementación del plan de tratamiento del riesgo
Verificar	Monitoreo y revisión continuo de los riesgos
Actuar	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

Los pasos que se siguen en el proceso de gestión del riesgo son (ICONTEC, 2009):

- **Establecimiento del Contexto:** Consiste en establecer el contexto para la gestión del riesgo en la seguridad de la información, lo que implica establecer los criterios básicos que son necesarios para la gestión del riesgo en la seguridad de la información, definir el alcance y los límites y establecer una organización adecuada que opere la gestión del riesgo de la seguridad de la información.

- **Valoración del Riesgo:** Consiste en identificar los riesgos, describirlos cuantitativa o cualitativamente y priorizarlos frente a los criterios de evaluación del riesgo y los objetivos relevantes para la organización. Se compone del análisis del riesgo, que a la vez se compone de la identificación y de la estimación del riesgo, y de la evaluación del riesgo:

    - **Identificación del Riesgo:** El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida. Para ello se deben identificar: los activos, las amenazas, los controles existentes, las vulnerabilidades y las consecuencias.

    - **Estimación del Riesgo:** El análisis del riesgo se puede realizar con diferentes grados de detalle dependiendo de la criticidad de los activos, la amplitud de las vulnerabilidades

conocidas y los incidentes anteriores que implicaron a la organización. Una metodología de estimación puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias. En la práctica, con frecuencia se utiliza la estimación cualitativa en primer lugar para obtener una indicación general del nivel del riesgo y revelar los riesgos más importantes. Posteriormente puede ser necesario realizar un análisis más específico o cuantitativo de los riesgos importantes dado que es, por lo general, menos complejo y menos costoso realizar un análisis cualitativo que uno cuantitativo.

- **Evaluación del Riesgo:** Consiste en comparar los niveles de riesgo frente a los criterios para la evaluación del riesgo y sus criterios de aceptación.

- **Tratamiento del Riesgo:** Consiste en seleccionar controles para reducir, retener, evitar o transferir los riesgos y se debería definir un plan para tratamiento del riesgo. Aquí entra en escena la prevención de los riesgos cuando se trata de evitar los riesgos.

- **Aceptación del Riesgo:** Consiste en tomar la decisión de aceptar los riesgos y las responsabilidades de la decisión, y registrarla de manera formal.

4.5.1.5 CRAMM: Método de Análisis y Gestión de Riesgos

Según Quasem (Qasem, 2013), CRAMM (*CCTA*[6] *Risk Analysis and Management Method*) ofrece un enfoque por etapas y disciplinado que abarca aspectos tanto técnicos como no técnicos de seguridad. Se divide en tres etapas:

- **Identificación de activos y valoración**: CRAMM permite identificar los activos físicos, el software, los datos y su ubicación, que conforman el sistema de información. Cada uno de estos activos puede ser valorado. Los activos físicos se valoran en términos del costo de reposición[7]. Los activos de datos y software se valoran en términos del impacto causado si la información no estuviera disponible, fuera destruida, divulgada o modificada.

- **Evaluación de amenazas y vulnerabilidades**: Habiendo comprendido la magnitud de los problemas potenciales, la siguiente etapa consiste en identificar la probabilidad de que este tipo de problemas se produzca. CRAMM cubre toda la gama de amenazas, deliberadas o

[6] CCTA: *Central Communication and Telecommunication Agency*

[7] **Costo de reposición:** Es el costo de reemplazar los activos de una compañía por una propiedad del mismo o igual valor. El costo de reposición del activo de una compañía puede ser un edificio, suministros, cuentas por cobrar o gravámenes. Este costo puede cambiar dependiendo de los cambios en el mercado de valores (INVESTOPEDIA).

accidentales, que pueden afectar a los sistemas de información, incluyendo: piratería, virus, fallas de equipos, etc.

- **Selección de contramedidas y recomendaciones**: CRAMM utiliza la evaluación de los riesgos de la etapa anterior y la compara con el nivel de seguridad requerido, con el fin identificar si los riesgos son lo suficientemente grandes como para justificar la instalación de una contramedida particular. Es en esta etapa donde tiene lugar la prevención de riesgos. CRAMM ofrece una serie de servicios de ayuda incluyendo: deshacer, qué pasa si?, funciones de priorización y herramientas de reportes para ayudar en la aplicación de contramedidas y la gestión activa de los riesgos identificados.

4.5.1.6 MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

En España, el Consejo Superior de Administración Electrónica (Consejo de Administración Electrónica) estableció la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) con el objetivo de implementar un marco común para el análisis y gestión de riesgos en los sistemas de información sobre la base de la norma ISO/IEC 27000. Esta metodología propone las siguientes etapas (Villalba, 2002):

- **Etapa 1. Planeación del Análisis y Gestión de Riesgos :** Esta etapa establece las consideraciones necesarias para iniciar el análisis de riesgos y el proyecto de gestión; permitiendo investigar si es apropiado llevarlo a cabo, definir los objetivos que debe cumplir y su dominio (alcance), determinar los recursos materiales y humanos necesarios para llevarlo a cabo y poner en marcha el proyecto.

- **Etapa 2. Análisis de Riesgos:** Esta etapa permite identificar y evaluar los elementos que intervienen en el riesgo para obtener una evaluación del riesgo en las diferentes áreas del dominio, y estimar los umbrales de riesgo deseables.

- **Etapa 3. Gestión de Riesgos:** Esta etapa permite identificar las funciones o servicios salvaguardias potenciales que reducen el riesgo detectado, para seleccionar las contramedidas adecuadas en función de aquellas que ya están implementadas y las restricciones dadas, simulando luego diferentes combinaciones de las mismas para especificar finalmente las seleccionadas.

- **Etapa 4. Selección de Salvaguardias:** Esta etapa permite seleccionar las contramedidas a implementarse, diseñando un enfoque para la aplicación de las salvaguardias seleccionadas; estableciendo los mecanismos para el seguimiento de su implementación, compilando los documentos de trabajo para el análisis de riesgos y el proceso de gestión, obteniendo los documentos finales del proyecto y haciendo presentaciones de los resultados en los diferentes niveles. Es en esta etapa que tiene lugar la prevención de riesgos.

4.5.1.7 Metodología de Gestión de Riesgos para Sistemas de Tecnologías de la Información según NIST

Esta guía NIST (*National Institute of Standards and Technology* - Instituto Nacional de Estándares y Tecnología) proporciona las bases para el desarrollo de un programa de gestión de riesgos efectivo, que contiene tanto las definiciones como las orientaciones prácticas necesarias para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI (Tecnologías de Información) (NIST, 2001). El objetivo fundamental es ayudar a las organizaciones a gestionar mejor los riesgos de TI relacionados con su misión. La evaluación de riesgos es el primer proceso dentro de esta metodología de gestión de riesgos. Las organizaciones utilizan la evaluación de riesgos para determinar el alcance de las amenazas potenciales y el riesgo asociado al sistema de TI a través de su SDLC (*System Development Life Cycle* – Ciclo de Vida de Desarrollo del Sistema). La salida de este proceso ayuda a identificar los controles adecuados para reducir o eliminar los riesgos durante el proceso de mitigación.

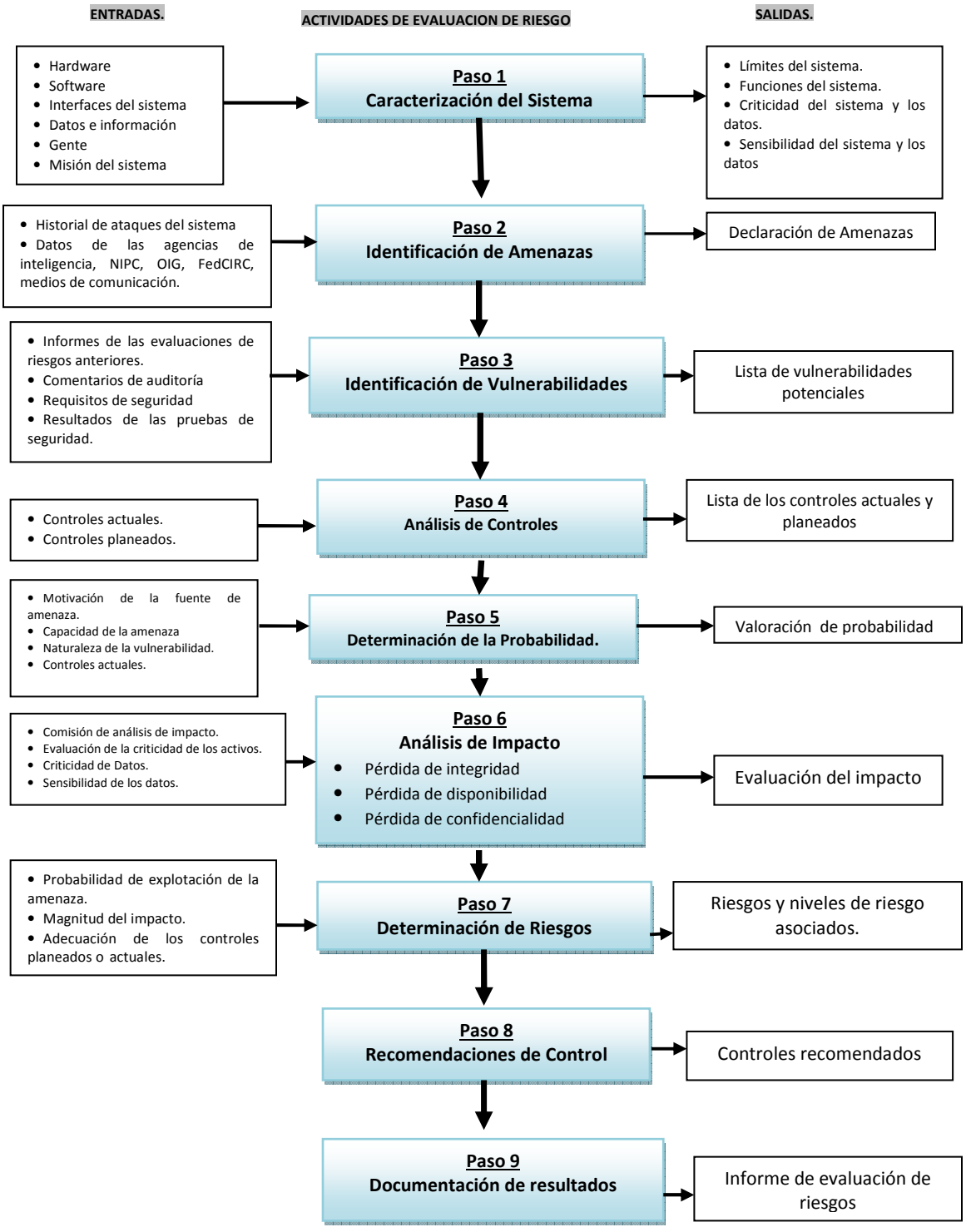

Figura 11: Organigrama de Metodología de evaluación de riesgo
Fuente: Risk Management Guide for Information Technology Systems (NIST, 2001)

Esta guía tiene 9 pasos definidos así (NIST, 2001) (ver Figura 11):

- **Paso 1- Caracterización del Sistema:** En este paso se identifican los límites del sistema TI, junto con los recursos y la información que lo constituyen. La caracterización del sistema TI establece el alcance de los esfuerzos de evaluación de riesgos, delinea los límites de la autorización operacional (o acreditación), y provee información (p.e. hardware, software, conectividad del sistema, división responsable o personal de soporte) esencial para definir el riesgo.

- **Paso 2- Identificación de Amenazas:** Un riesgo es el potencial de que una fuente de amenaza particular explote exitosamente una vulnerabilidad particular. Una vulnerabilidad es una debilidad que puede ser accidentalmente activada o intencionalmente explotada. Una fuente de amenaza no representa un riesgo cuando no hay una vulnerabilidad que pueda ser explotada. Para determinar la probabilidad de una amenaza, se pueden considerar las fuentes de amenaza, las vulnerabilidades potenciales y los controles existentes.

- **Paso 3- Identificación de Vulnerabilidades:** El análisis de amenazas a un sistema TI debe incluir un análisis de las vulnerabilidades asociadas con el entorno del sistema. El objetivo de este paso es crear una lista de las vulnerabilidades del sistema (fallas o debilidades) que pueden ser explotadas por las fuentes potenciales de amenaza.

- **Paso 4- Análisis de Controles:** El objetivo de este paso es analizar los controles implementados o que planea implementar la organización, para minimizar o eliminar la probabilidad de que una amenaza explote una vulnerabilidad del sistema. Existen dos categorías de controles:
    - Los controles preventivos, que evitan los intentos de violar las políticas de seguridad e incluyen el control de ejecución, el cifrado y la autenticación
    - Los controles de detección, que alertan sobre violaciones o intentos de violaciones de las políticas de seguridad e incluyen auditorías de rastreo, métodos de detección de intrusión, y control de errores.

- **Paso 5- Determinación de la Probabilidad:** Para obtener una tasa de probabilidad general que indique la probabilidad que una vulnerabilidad potencial pueda ser explotada dentro de la construcción del entorno de amenazas asociado, se pueden considerar los siguientes factores:

    - Motivación y capacidad de la fuente de amenaza
    - Naturaleza de la vulnerabilidad
    - Existencia y efectividad de los controles actuales

  La probabilidad de que una vulnerabilidad sea explotada por una fuente de amenaza puede ser: alta (la fuente de amenaza está altamente motivada y es suficientemente capaz, y los controles para prevenir que la vulnerabilidad sea explotada son inefectivos); media (la fuente de amenaza está motivada y es capaz, pero los controles implementados pueden impedir que se explote exitosamente la vulnerabilidad), baja (la fuente de amenaza no está motivada o no es capaz o se han implementado controles para prevenir, o al menos impedir significativamente, que la vulnerabilidad sea explotada).
- **Paso 6- Análisis del Impacto:** Este paso consiste en medir el nivel de riesgo para determinar el impacto adverso que resulta de la explotación exitosa de una vulnerabilidad por una amenaza. Antes de iniciar el análisis del impacto es necesario obtener la siguiente información:

- Misión del sistema (es decir, los procesos desarrollados por el sistema TI)
- Criticidad del sistema y de los datos (es decir, el valor del sistema o su importancia para la organización)
- Sensibilidad del sistema y de los datos

El impacto adverso de un sistema de seguridad puede describirse en términos de la pérdida o degradación de uno o una combinación, de los siguientes objetivos de seguridad: integridad, disponibilidad y confidencialidad.

- **Paso 7- Determinación de Riesgos:** Este paso consiste en evaluar el nivel de riesgo del sistema TI. La determinación del riesgo para una pareja particular amenaza/vulnerabilidad puede ser expresada en función de:

  - La probabilidad de que un intento de amenaza dado explote una determinada vulnerabilidad
  - La magnitud del impacto cuando una amenaza explota exitosamente una vulnerabilidad
  - La idoneidad de los controles de seguridad planeados o existentes para reducir o eliminar los riesgos.

  Se debe obtener la medida del riesgo, la escala del riesgo y la matriz de nivel del riesgo.

- **Paso 8- Recomendaciones de Control:** Durante este paso, se determinan los controles apropiados para las operaciones de la organización, que pueden mitigar o eliminar los riesgos identificados. El objetivo de los controles recomendados es reducir el nivel de riesgo del sistema TI y sus datos a un nivel aceptable. Los siguientes factores deberían considerarse al recomendar controles y soluciones alternativas para minimizar o eliminar los riesgos identificados:

  - Efectividad de las opciones recomendadas (es decir, compatibilidad del sistema)
  - Legislación y regulación
  - Política organizacional
  - Impacto operacional
  - Seguridad y confiabilidad

  Las recomendaciones de control son el resultado del proceso de evaluación del riesgo y proporciona la entrada al proceso de mitigación de riesgos, durante el que los controles procedimentales y de seguridad técnica recomendados son evaluados, priorizados e implementados. En este paso se plantean las estrategias de prevención.

- **Paso 9- Documentación de Resultados:** Una vez que la evaluación del riesgo se ha completado (se han identificado las fuentes de amenaza y vulnerabilidades, se han evaluado los riesgos y se han recomendado controles), los resultados deben ser documentados en un reporte oficial o instrucciones.

Un reporte de evaluación de riesgos es un reporte de gestión que ayuda a la alta gerencia a tomar decisiones respecto a las políticas, procedimientos, presupuesto y cambios en el sistema operacional y de gestión. Diferente a un reporte de auditoría o investigación que se centra en lo que se está haciendo mal, un reporte de evaluación de riesgos no debe presentarse de una manera acusatoria sino con un enfoque sistemático y analítico de evaluación del riesgo para que la alta gerencia entienda los riesgos y destine recursos para reducir y corregir las pérdidas potenciales. Por esta razón, algunas personas prefieren tomar las parejas amenaza/vulnerabilidad como observaciones en lugar de como hallazgos del reporte de evaluación de riesgos.

Esta guía recomienda la integración de la evaluación de riesgos en el SDLC (NIST, 2001). La evaluación de riesgos es un proceso iterativo que se puede realizar durante cada una de las fases principales del SDLC. Esto indica que el proceso de evaluación de riesgos debe estar integrado en la primera fase del SDLC, es decir, en la fase de requerimientos. La metodología tiene pasos muy simples y es muy fácil desde la perspectiva de implementación.

4.5.2 METODOLOGÍAS DE PREVENCIÓN

4.5.2.1 Metodología para el Diagnóstico, Prevención y Control de la Corrupción en Programas de Seguridad Ciudadana según el BID

Esta metodología fue elaborada por un equipo de trabajo del Banco Interamericano de Desarrollo (BID). Parte de la correlación entre la seguridad ciudadana y la corrupción, y se basa en el análisis de la cadena de valor.

Aunque esta metodología no habla en sí de la seguridad informática, si aborda la prevención desde el punto de vista de la problemática social, lo que es de gran contribución para este proyecto, ya que no se deben considerar solo los factores tecnológicos sino también los sociales, y puede adaptarse al entorno que nos ocupa.

El concepto de cadena de valor consiste en la identificación de los principales procesos que aportan más a la generación de valor en una organización o programa. Mientras que en el modelo tradicional las diversas actividades que la institución ejecuta se agrupan de acuerdo con su naturaleza (contables, comerciales, técnicas, etc.), en el modelo de procesos estas mismas actividades se reagrupan en función de su papel en la creación de valor. Se dividen en dos tipos: actividades primarias o críticas, que son las que contribuyen directamente a la creación de valor; y actividades administrativas o de soporte, que son aquellas que sustentan el desarrollo de las actividades primarias.

Para diseñar la cadena de valor de los programas de seguridad ciudadana se han identificado las diversas tareas que se deben ejecutar en cada uno de sus estamentos para el cabal cumplimiento de los objetivos, funciones y restricciones. Estas tareas se han desagregado en dos niveles, denominados macro-procesos y sub procesos. Cada uno de los sub procesos está dividido en actividades. Los macro procesos críticos de la cadena de valor de la seguridad ciudadana son :

(i) **Desarrollar Políticas de Seguridad:** Consiste en articular la respuesta pública a las demandas y necesidades sociales de seguridad ciudadana.

(ii) **Prevenir la violencia:** Es contrarrestar los factores multidimensionales que aumentan los riesgos de criminalidad y victimización.

(iii) **Controlar y sancionar:** Es asegurar el respeto de la ley y el orden público, proteger a las personas y bienes ante la amenaza de delitos, de ser el caso, aplicando las consecuencias jurídicas derivadas del incumplimiento de la Ley.

(iv) **Rehabilitar y reinsertar a la sociedad:** Es tratar y rehabilitar a la población reclusa o menores de edad que han infringido la ley (prevención terciaria) para su reinserción social, así como a las víctimas de delitos.

(v) **Supervisar y Evaluar las Políticas:** Monitorear, supervisar y evaluar el cumplimiento de la misión, objetivos y metas establecidos en los planes y actividades de manera ordenada y eficiente.

Cada uno de estos macro procesos implica llevar a cabo los siguientes pasos :

- **Identificación y Análisis de los Riesgos:** Consiste en identificar los riesgos de cada uno de los principales procesos identificados, así como su nivel, entendido éste como la probabilidad de ocurrencia y el impacto que generaría en caso de materializarse. El impacto del riesgo varía en cada proyecto, por lo que debe ser analizado caso por caso.
  Para analizar la presencia de un determinado riesgo, se utiliza un conjunto de indicadores que contribuyen a determinar objetivamente si existe o no la posibilidad de ocurrencia de un riesgo determinado, así como las posibles consecuencias (impacto) que este tendría de realizarse. Los indicadores miden la presencia de la buena práctica a nivel normativo y luego su nivel de implementación real, lo que da una aproximación más precisa de donde está la brecha y de las alternativas de solución más precisas.

- **Respuesta a los Riesgos:** Una vez identificados los riesgos de cada uno de los procesos, es posible identificar un abanico de alternativas de respuesta a estos. Es claro que la alternativa seleccionada dependerá de las características propias de cada situación en particular, por lo que se ofrecen simplemente al tomador de decisiones un conjunto de alternativas de medidas que pueden ser respuestas efectivas a los riesgos. Por tanto, se puede seleccionar una o una combinación de éstas acciones que puedan dar una respuesta efectiva a los riesgos identificados. Para llevar a cabo esta respuesta a los riegos se consideraron:

    - **Dimensiones de análisis:** Se tuvieron en cuenta dos dimensiones de análisis, para construir la lista de respuestas a los riesgos.
      En primer lugar, las respuestas a los riesgos pueden ser de dos tipos: transversales y específicas. Las primeras son válidas para prevenir todos los riesgos a la corrupción, cualquiera que sea su modalidad y ubicación en la cadena de valor, sea o no una de las áreas o procesos especialmente vulnerables. Las segundas tienen por objeto prevenir manifestaciones específicas de la corrupción. Estas últimas son la adaptación a un riesgo específico de las medidas transversales.
      En segundo lugar, se han tenido en cuenta las categorías estratégicas de respuesta a los riesgos sugeridas por el PMI (*Project Management Institute*), principalmente Evitar y Mitigar (PMI, 2008). Evitar implica modificar el programa de manera que el riesgo se elimine por completo. La forma más radical de evitar el riesgo sería cerrar el programa

por completo. Sin embargo, como los riesgos pueden afectar de manera distinta a cada proceso, es posible también cancelar algún proceso u objetivo determinado que es más susceptible al riesgo y no se encuentran medidas de eliminación o mitigación aceptables. Por su parte, mitigar implica reducir la probabilidad de ocurrencia o el impacto de un riesgo dentro de un límite aceptable para las organizaciones. También se ha considerado la posibilidad de diseñar respuestas para desarrollarse en caso de que un riesgo se materialice, por lo que toman la forma de planes de contingencia.

Finalmente, se ha tenido en cuenta que en algunos casos las respuestas a los riesgos pasan por introducir reformas a otros procesos de la cadena de valor, no directamente al proceso en riesgo, pues el origen del riesgo está en otro proceso.

- **Revisión de las Alternativas Disponibles:** La literatura discute extensamente las responsabilidades individuales, institucionales y sociales en la corrupción. Existe, en general, acuerdo en que es necesario contar con políticas de probidad que incidan en estos tres niveles, aunque desde el Estado es mucho más fácil actuar en relación con las dos primeras, es decir, los servidores públicos y la cultura de las instituciones. Asuntos tales como el diseño institucional y la cultura organizacional son fundamentales para entender los hechos de corrupción. Dentro de esta lógica, tan o más importante como reclutar a gente proba será contar con instituciones cuyo diseño y cultura estén alineadas firmemente con la lucha contra la corrupción. Esto es especialmente importante en la cadena de valor de la seguridad ciudadana, considerando que las instituciones que forman parte de ella, especialmente las policiales y penitenciarias, están de manera permanente asociadas a quienes viven de la actividad criminal, para quienes neutralizar su acción resulta fundamental.

  Desde esta perspectiva, la lucha contra la corrupción no puede ser solo ni principalmente un esfuerzo por identificar y castigar a los corruptos, lo que en cualquier caso es necesario e imprescindible, sino por identificar los patrones de la corrupción, esto es, sus áreas más vulnerables y sus principales manifestaciones, con el propósito de modernizar la gestión institucional para reducir la discrecionalidad de los servidores públicos, transparentar su actuación y hacerlos responsables de sus actos (E. Campos & Pradhan, 2007).

  La respuesta a la corrupción tiene gran incidencia en los procesos de apoyo, toda vez que son transversales y dan soporte a todos los procesos críticos. Es decir, su implementación evita o mitiga una amplia diversidad de riesgos que se manifiestan en los procesos críticos.

4.5.2.2 Metodología de Prevención de Incidentes de Malware según NIST

Para esta metodología, el *National Institute of Standards and Technology* (NIST) considera que los cuatro elementos principales de la prevención son: las políticas, la concientización, la mitigación de vulnerabilidades y la mitigación de amenazas. Las políticas dirigidas a la prevención del malware son la base para implementar controles preventivos. Establecer y mantener programas generales de concientización sobre el malware para todos los usuarios, así como programas de entrenamiento específico en concientización para el personal de TI directamente involucrado en las actividades de prevención de incidentes, es crítico para reducir el número de incidentes que ocurren por errores humanos. Invertir esfuerzos en la mitigación de vulnerabilidades puede eliminar algunos posibles vectores de ataque. Implementar una combinación de técnicas y herramientas de mitigación de amenazas, como software antivirus y cortafuegos, puede prevenir

las amenazas que atacan exitosamente los diferentes sistemas y redes. A continuación se describe cada uno de estos elementos en detalle pues las organizaciones deben crear una guía de recomendaciones para cada categoría a fin de crear una defensa en capas efectiva contra el malware. Sin embargo, las organizaciones deben ser conscientes que sin importar el esfuerzo que pongan en la prevención de incidentes de malware, los incidentes aún ocurrirán (por ejemplo, por tipos de amenazas desconocidos, errores humanos, etc.) (Mell et al., 2005):

- **Políticas:** Las organizaciones deben asegurar que sus políticas se dirigen a la prevención de incidentes de malware. Estas políticas deben ser usadas como la base para esfuerzos adicionales de prevención de malware, tales como la concientización de los usuarios y del personal de TI, la mitigación de vulnerabilidades y la mitigación de amenazas. Si una organización no establece claramente las consideraciones de prevención del malware en sus políticas, es improbable que lleve a cabo actividades de prevención del malware consistentes y efectivas a lo largo de la organización. Las políticas relacionadas con la prevención del malware deben ser tan generales como sea posible para proveer flexibilidad en la implementación de estas políticas y reducir la necesidad de frecuentes actualizaciones de las mismas, pero también deben ser lo suficientemente específicas para que el propósito y el alcance de las políticas sean claros. Las políticas de prevención del malware deben incluir cláusulas relacionadas con los trabajadores remotos que usen sistemas controlados por la organización y sistemas no contralados por la organización (por ejemplo, computadores de los contratistas, computadores en la casa de los empleados, computadores de los compañeros de negocios, dispositivos móviles)

- **Concientización:** Un programa de concientización efectivo explica las reglas apropiadas de comportamiento para el uso de los sistemas de TI y de información de la organización. Por tanto, los programas de concientización deberían incluir una guía para los usuarios sobre la prevención de los incidentes de malware, que pueda ayudar a reducir la frecuencia y severidad de estos incidentes. Todos los usuarios de una organización deberían ser conscientes de las maneras en que entra el malware a los sistemas, los infecta y se expande; los riesgos que supone el malware; la inhabilidad de los controles técnicos para prevenir todos los incidentes y la importancia de que los usuarios prevengan estos incidentes. Las actividades de concientización también deben tener en cuenta las características de los diferentes entornos, como aquellas encontradas por los tele-trabajadores y empleados viajeros en hoteles, cafeterías y otras locaciones externas. Además, el programa de concientización de la organización debe cubrir las consideraciones de prevención de incidentes de malware indicados en las políticas y procedimientos de la organización. También, las organizaciones deben dar a conocer a los usuarios las políticas y procedimientos a aplicar para manejar los incidentes de malware, como: cómo identificar si un sistema puede estar infectado, cómo reportar una sospecha de infección y qué pueden hacer los usuarios para ayudar a manejar el incidente (p.e. actualizar el antivirus, escanear el sistema en busca de malware).

- **Mitigación de Vulnerabilidades:** Usualmente, una vulnerabilidad puede ser mitigada mediante uno o más métodos como aplicando parches de actualización al software, o reconfigurando el software (p.e. reconfigurando un servicio vulnerable). Debido a los desafíos que presenta la mitigación de vulnerabilidades, incluyendo el continuo descubrimiento de nuevas vulnerabilidades, las organizaciones deben tener documentados las políticas, procesos y procedimientos para la mitigación de vulnerabilidades y deberían también considerar, la creación de un programa de gestión de vulnerabilidades que ayude en las tareas de mitigación. También se deben evaluar constantemente las vulnerabilidades, para que las tareas de mitigación sean priorizadas apropiadamente. Además, deben contar con un método de seguimiento del progreso de las tareas de mitigación. Las organizaciones deberían usar el principio de defensa en capas para mitigar las vulnerabilidades ya que una medida simple no será suficiente para mitigar todas las vulnerabilidades. Las técnicas de mitigación de vulnerabilidades pueden dividirse en 3 categorías generales:
    - **Gestión de parches:** Es la forma más común de mitigar las vulnerabilidades en los sistemas operativos y aplicaciones. Esta involucra muchos pasos como: la evaluación de la criticidad de los parches y el impacto de aplicarlos o no, el testeo completo de los parches, aplicar los parches de una manera controlada y documentar la evaluación del parche y el proceso de decisión.
    - **Quitar privilegios:** Se refiere a configurar los sistemas para otorgar solo los derechos mínimos a los usuarios, procesos y *hosts* apropiados. Este puede minimizar la magnitud del daño causado por el malware.
    - **Otras medidas de fortalecimiento de los *hosts*:** Para reducir la probabilidad de incidentes de malware, como: deshabilitar o quitar servicios innecesarios, eliminar la compartición de archivos insegura, remover o cambiar los nombres de usuarios y contraseñas por defecto de los sistemas operativos y aplicaciones, solicitar autenticación antes de permitir el acceso a los servicios de red, deshabilitar la reproducción automática de archivos binarios y scripts.
- **Mitigación de Amenazas:** Las organizaciones deben realizar la mitigación de amenazas para detectar y parar el malware antes de que afecte a sus objetivos. Existen, muchos tipos de herramientas de seguridad que pueden mitigar las amenazas de malware:
    - **Software antivirus:** Para los sistemas operativos y las aplicaciones que son objeto frecuente del malware, el software antivirus se ha convertido en una necesidad para prevenir los incidentes. Se recomienda que un antivirus sea capaz de: escanear los componentes críticos del sistema; vigilar las actividades en tiempo real de los sistemas, para detectar actividades sospechosas; monitorear el comportamiento de las aplicaciones comunes, como clientes de correo y navegadores web; escanear los archivos en busca de virus; identificar los tipos comunes de malware (virus, gusanos,

troyanos, código móvil malicioso, amenazas mezcladas), así como las herramientas de ataque; y desinfectar los archivos.

- **Detección de spyware y utilidades de remoción:** Se diseñan para identificar muchos tipos de spyware en los sistemas y para colocar en cuarentena o remover archivos spyware.

- **Sistemas de prevención de intrusos:** Los sistemas de prevención de intrusos (IPS) basados en red realizan captura de paquetes y analizan el tráfico de red para identificar y parar las actividades sospechosas. Los IPS basados en red actúan como *firewall* de red, pues reciben paquetes, los analizan, deciden si deben ser aceptados, y les permiten a los paquetes aceptados pasar. Esta arquitectura permite detectar algunos ataques en la red antes de que alcancen sus objetivos. Muchos IPS basados en red usan una combinación de firmas de ataque y análisis de la red y de los protocolos de aplicación, lo que significa que comparan la actividad en la red de las aplicaciones atacadas frecuentemente (p.e. servidores de correo electrónico, servidores web) con el comportamiento esperado para identificar actividad maliciosa potencial.

- ***Firewalls* y *routers*:** Dispositivos de red tales como los *firewalls* y los *routers*, examinan el tráfico de red y lo permiten o deniegan de acuerdo a un conjunto de reglas. Un *router* usa un conjunto simple de reglas conocido como lista de control de acceso (ACL), que sólo dirigen las características más básicas del tráfico de red, mientras que los *firewalls* ofrecen capacidades más robustas. Existen dos tipos de *firewall*: *firewall* de red y *firewall* basados en *host*. Un *firewall* de red se coloca entre las redes para restringir qué tipo de tráfico puede pasar de una red a otra. Un *firewall* basado en *host* es un software que corre en un simple *host* que puede restringir la actividad de red entrante y saliente de dicho *host*.

- **Configuración de aplicaciones:** La configuración por defecto de las aplicaciones tiende a favorecer la funcionalidad sobre la seguridad. Por eso, las organizaciones deberían deshabilitar las características y capacidades innecesarias de las aplicaciones, particularmente aquellas que son comúnmente explotadas por el malware. Algunas configuraciones de aplicaciones a considerar en la prevención de incidentes de malware son: bloquear archivos adjuntos sospechosos en los correo electrónicos, filtrar el *spam*, filtrar el contenido web, limitar la ejecución de código móvil, restringir las *cookies* del navegador web, bloquear las ventanas *popup* del navegador web, prevenir la instalación de software en los navegadores web, prevenir la carga automática de las imágenes de los correos electrónicos, alterar las asociaciones de archivos, restringir el uso de macros, prevenir la apertura de correos masivos.

4.6 COMPARACIÓN DE METODOLOGÍAS

Ya que se van a comparar diferentes metodologías, se va a establecer un paralelo entre las fases o pasos que estas incluyen. Se han identificado cuatro fases básicas, que se repiten en casi todas las metodologías:

1. **Establecer el contexto:** Consiste en identificar los activos importantes para la organización, los requisitos de seguridad de esos activos, lo que la organización está haciendo para proteger sus activos, y los objetivos que se persiguen con el análisis de riesgos.
2. **Identificar los riesgos**: Consiste en determinar qué vulnerabilidades poseen los diferentes activos e identificar las amenazas que pueden explotarlas.
3. **Analizar los riesgos:** Consiste en calcular la probabilidad que una amenaza explote una determinada vulnerabilidad y establecer el nivel de riesgo de cada activo, priorizándolos para tomar acciones posteriormente.
4. **Tratar los riesgos:** Consiste en implantar contramedidas que permitan evitar, mitigar, aceptar o transferir los riesgos.

La comparación va a consistir en determinar si las diferentes metodologías incluyen estas fases y establecer si se enfocan en una fase determinada o si especifican claramente lo que se hace en cada fase. También, se va a determinar si estas metodologías consideran el factor humano dentro de sus diferentes pasos, ya que el ser humano es el eslabón más débil de la cadena de la seguridad (Lizarazo Rueda, 2012).

En la Tabla 4 se muestra el cuadro comparativo de las diferentes metodologías, indicando si incluyen las fases identificadas anteriormente.

Tabla 4. Comparación de Metodologías

FASE	METODOLOGÍAS DE GESTIÓN DE RIESGOS							METODOLOGÍAS DE PREVENCIÓN DE RIESGOS	
	OCTAVE	**CORAS**	**Metodología de Administración de Riesgos según Estándar Australiano**	**NTC-ISO/IEC 27005: Gestión del Riesgo en la Seguridad de la Información**	**CRAMM**	**MAGERIT**	**Metodología de Gestión de Riesgos para Sistemas de Tecnologías de la Información según NIST**	**Metodología para el Diagnóstico, Prevención y Control de la Corrupción en Programas de Seguridad Ciudadana según el BID**	**Metodología de Prevención de Incidentes de Malware según NIST**
Establecer el contexto	Corresponde a la Fase 1. Construir Perfiles de Amenazas Basados en Activos	Corresponde a los 3 primeros pasos: Paso 1. Introducción Paso 2. Análisis de Alto Nivel Paso 3. Aprobación	Corresponde a la Fase 1. Establecer el contexto	Corresponde al Paso 1. Establecimiento del contexto	Corresponde a la Etapa 1. Identificación de Activos y Valoración	Corresponde a la Etapa 1. Planeación del Análisis y Gestión de Riesgos	Corresponde al Paso 1. Caracterización del Sistema	N/A	N/A
Identificar los riesgos	Corresponde a las	Corresponde al Paso 4.	Corresponde a la Fase 2.	Corresponden al paso 2.	Corresponden a la Etapa 2.	Corresponden a la Etapa	Corresponde a los pasos 2, 3 y	Corresponden al Paso 1.	N/A

FASE	METODOLOGÍAS DE GESTIÓN DE RIESGOS							METODOLOGÍAS DE PREVENCIÓN DE RIESGOS	
	OCTAVE	**CORAS**	**Metodología de Administración de Riesgos según Estándar Australiano**	**NTC-ISO/IEC 27005: Gestión del Riesgo en la Seguridad de la Información**	**CRAMM**	**MAGERIT**	**Metodología de Gestión de Riesgos para Sistemas de Tecnologías de la Información según NIST**	**Metodología para el Diagnóstico, Prevención y Control de la Corrupción en Programas de Seguridad Ciudadana según el BID**	**Metodología de Prevención de Incidentes de Malware según NIST**
	Fases 1 y 2: Fase 1. Construir Perfiles de Amenazas Basados en Activos Fase 2. Identificar Vulnerabilidades de la Infraestructura	Identificación de Riesgos	Identificar Riesgos	Valoración del Riesgo	Evaluación de Amenazas y Vulnerabilidades	2. Análisis de Riesgos	4: Paso 2. Identificación de Amenazas Paso 3. Identificación de Vulnerabilidades Paso 4. Análisis de Controles	Identificación y Análisis de los Riesgos	
Analizar los Riesgos	Corresponden a la Fase 3. Desarrollar las Estrategias y los Planes de Seguridad	Corresponde a los Pasos 5 y 6: Paso 5. Estimación de Riesgos Paso 6. Evaluación de Riesgos	Corresponde a las Fases 3 y 4: Fase 3. Analizar Riesgos Fase 4. Evaluar Riesgos				Corresponde a los pasos 5, 6 y 7: Paso 5. Determinación de la Probabilidad Paso 6. Análisis del Impacto Paso 7. Determinación de Riesgos		N/A
Tratar los Riesgos		Corresponde al Paso 7. Tratamiento de Riesgos	Corresponde a la Fase 5. Tratar Riesgos	Corresponde a los pasos 3 y 4. Paso 3. Tratamiento del Riesgo Paso 4. Aceptación del Riesgo	Corresponde a la Etapa 3. Selección de Contramedidas y Recomendaciones	Corresponde a las etapas 3 y 4: Etapa 3. Gestión de Riesgos Etapa 4. Selección de Salvaguardias	Corresponde a los pasos 8 y 9: Paso 8: Recomendaciones de Control Paso 9. Documentación de Resultados	Corresponde al Paso 2. Respuesta a los Riesgos	Corresponde a los 4 elementos principales: Políticas, Concientización, Mitigación de Vulnerabilidades y Mitigación de Amenazas

Como se puede apreciar en la Tabla 4, la metodología OCTAVE aunque incluye las cuatro fases que se han definido para este análisis no presenta una división estricta de dichas fases. OCTAVE se centra principalmente en su primera fase donde se identifica primero el conocimiento y prácticas de seguridad de la alta gerencia, del área operacional, y del personal para construir posteriormente los diferentes perfiles de amenazas. Por tanto, en esta fase se tiene en cuenta el factor humano. La identificación de riesgos, se lleva a cabo en la primera y segunda fase de OCTAVE, porque en la primera fase establece los perfiles de amenazas y en la segunda identifica las vulnerabilidades, sin embargo, al determinar primero las amenazas y luego las

vulnerabilidades, no queda clara la correspondencia entre estas, pues se debe identificar qué amenazas pueden explotar una determinada vulnerabilidad. En esta fase de identificación de los riesgos no se considera explícitamente el factor humano sino los activos de la organización. La tercera fase de OCTAVE incluye tanto el análisis como el tratamiento de los riesgos, y tiene en cuenta el factor humano, porque en los procesos de esta fase se hace un análisis de riesgos de conducta y se fomenta la estrategia de protección en la organización, sin embargo, no se establecen estrategias específicas de protección y prevención.

En cuanto a la metodología CORAS, esta se basa en la realización de una serie de reuniones y talleres con diferentes fines, de acuerdo al paso que se esté realizando. Como se aprecia en la Tabla 4, esta metodología incluye las cuatro fases consideradas en este análisis. La fase de establecimiento del contexto, se lleva a cabo en los 3 primeros pasos de CORAS. En este caso, los analistas se basan en la información proporcionada por los representantes del cliente, por lo que no son ellos los que reúnen directamente la información que requieren de la empresa, lo que puede llevar a no contar con toda la información necesaria para realizar un análisis de riesgos completo. Sin embargo, se hacen en esta primera fase 3 reuniones para estar seguros que comprendieron adecuadamente la información presentada por el cliente. La fase de identificación de riesgos, se lleva a cabo en el cuarto paso de CORAS, donde se identifican los vulnerabilidades y los diferentes escenarios de amenaza a través de un taller con expertos en el objeto de análisis. La fase de análisis de riesgos, se lleva a cabo en los pasos 5 y 6 de CORAS, donde se obtienen los valores de probabilidad y un cuadro de riesgos general. La fase de tratamiento de riesgos, se lleva a cabo en el séptimo paso de CORAS, donde se determina qué tratamiento se va a dar a los riegos y se hace un análisis costo/beneficio. Ya que los analistas no tienen un contacto directo con el personal de la empresa cliente, esto puede llevar a descuidar el factor humano y a tener una visión errada de los procesos y prácticas de seguridad que se llevan a cabo en la misma, obteniendo resultados que pueden no adaptarse al contexto real de la empresa. No se establecen estrategias específicas de protección y prevención.

Según la Tabla 4, la Metodología de Administración de Riesgos del Estándar Australiano incluye las cuatro fases consideradas en este análisis. Esta metodología, se centra en las fases de identificación y análisis de riesgos, donde se incluyen todos los riesgos (estén o no bajo el control de la organización) y se analizan las fuentes y consecuencias de los mismos para calcular luego su probabilidad y establecer su nivel, de acuerdo a un análisis tanto cualitativo como cuantitativo. Sin embargo, el establecimiento del contexto se hace teniendo en cuenta el contexto estratégico, organizacional y de administración de riesgos, por lo que no se centra en el factor humano, sino en los objetivos que quiere alcanzar la organización. Tampoco se definen estrategias específicas de protección y prevención en la fase de tratamiento de los riesgos, aunque si establece un proceso cíclico de tratamiento de los mismos, lo que permite verificar si las contramedidas implementadas tienen el efecto esperado o si deben reemplazarse por otras.

La metodología de gestión de riesgos NTC-ISO /IEC 27005 incluye las cuatro fases consideradas en este análisis, pero no menciona específicamente el factor humano, pues sus pasos se describen de

manera muy general. Esta metodología tiene un interés particular en la valoración del riesgo donde se realiza la identificación, estimación y evaluación del mismo. Ya que la eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo, si la información que arroja este paso no es suficiente, se llevan a cabo tantas iteraciones como sean necesarias de valoración del riesgo con un contexto revisado, para poder realizar un tratamiento adecuado. Además, no se definen estrategias específicas de protección y prevención en el paso de tratamiento del riesgo.

El método de análisis CRAMM aunque incluye las cuatro fases consideradas en este análisis es bastante general y no se centra en ninguna de estas fases. Tampoco habla específicamente del factor humano ni define estrategias específicas de protección y prevención. La etapa de identificación de activos y valoración de CRAMM se centra solo en los activos físicos y de información, aunque en la etapa de evaluación de amenazas y vulnerabilidades si dice que se consideran todas las amenazas deliberadas o accidentales, por lo que aquí podría estar implícito el factor humano.

La metodología MAGERIT es también bastante general en la descripción de sus etapas, aunque incluye las cuatro fases consideradas en este análisis. En la etapa de planeación del análisis y gestión de riesgos considera los recursos humanos pero para llevar a cabo el análisis de riesgos, no habla en sí del factor humano de la organización. Además, en la etapa de análisis de riesgos, no se especifica qué tipos de amenazas se consideran ni cómo se determinan los umbrales de riesgo deseables. MAGERIT se centra principalmente en la etapa de gestión de riesgos donde simula diferentes combinaciones de salvaguardias para seleccionar las que más se acomoden al contexto de la organización, y luego en la etapa de selección de salvaguardias, hace un seguimiento a la implementación de estas salvaguardias, las documenta y las da a conocer en los diferentes niveles de la organización, así que por lo menos en esta etapa se tiene en cuenta el factor humano. No define estrategias específicas de protección y prevención.

La Metodología de Gestión de Riesgos según NIST, es quizás la metodología más completa de todas las estudiadas, ya que incluye las cuatro fases consideradas en este análisis y proporciona tanto las definiciones como las orientaciones prácticas necesarias para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI, por lo que describe de una manera muy precisa lo que se debe hacer en cada uno de sus 9 pasos. Esta metodología también considera el factor humano, pues tiene en cuenta la motivación de las diferentes fuentes de amenazas y esta ayuda a determinar la probabilidad del riesgo. Además, considera los controles tanto preventivos como correctivos.

Las Metodologías de Prevención de Riesgos ofrecen un panorama centrado en el análisis de riesgos y sobretodo en el tratamiento de los mismos. La Metodología para el Diagnóstico, Prevención y Control de la Corrupción en Programas de Seguridad Ciudadana según el BID, aunque no es una metodología orientada a los sistemas de TI, es muy interesante para este estudio pues se centra en el factor humano, considerando la cadena de valor de los diferentes procesos que se llevan a cabo en una organización y las responsabilidades individuales, institucionales y sociales, a

la hora de implementar los controles preventivos. En esta metodología la identificación y el análisis de los riesgos se hacen de manera más cualitativa que cuantitativa, mientras en la respuesta a los riesgos se consideran varias dimensiones de análisis y se revisan las alternativas disponibles. La Metodología de Prevención de Incidentes de Malware según NIST, por su parte, incluye solamente la fase del tratamiento de los riesgos, estableciendo los cuatro elementos principales de la prevención: las políticas, la concientización, la mitigación de vulnerabilidades y la mitigación de amenazas. En la concientización es donde incluye el factor humano, y describe los aspectos a tener en cuenta para implementar los cuatro elementos de prevención.

Además, algo se evidenció en todas las metodologías al explorar sus lineamientos es la complejidad en la descripción de lo que se debe realizar en cada paso, pues suelen contar con diferentes anexos que buscan aclarar los diferentes pasos, pero que terminan por confundir al lector.

5 METODOLOGÍA DE PREVENCIÓN DE RIESGOS PARA SISTEMAS DE INFORMACIÓN ACADÉMICA (MEPRISIA)

5.1 CONSIDERACIONES INICIALES

Como se evidenció en el análisis de las metodologías de gestión y prevención de riesgos estudiadas en la unidad anterior, muchas de ellas no especifican la inclusión del factor humano en cada uno de sus pasos, lo que es muy importante puesto que los seres humanos son el eslabón más débil en la cadena de la seguridad (Lizarazo Rueda, 2012). Además, la complejidad en la descripción de los pasos de dichas metodologías dificulta su implementación. Por dichas razones, consideramos que los factores que deben diferenciar a la metodología de prevención de riesgos diseñada en este trabajo de grado deben ser: la claridad en la descripción de cada paso, lo que ayudará a facilitar su implementación, y la inclusión del factor humano.

Esta metodología tendrá además en cuenta los cuatro pasos o fases identificadas en el análisis de las metodologías.

5.2 METODOLOGÍA

5.2.1 INTRODUCCIÓN

El riesgo es la probabilidad de que un evento adverso ocurra y afecte a un sistema de información y a sus activos asociados (personas, información, infraestructura) como resultado de la combinación de una amenaza de seguridad y una vulnerabilidad, causando pérdidas o daños a la organización (fallas en el funcionamiento de los equipos; mal funcionamiento de las aplicaciones; robo, modificación y/o pérdida de información; mala imagen pública, demandas, etc.). Debido al efecto adverso de los riesgos, las instituciones educativas deberían implementar medidas de seguridad que ayuden a prevenir que estos se presenten. En este documento se presenta una Metodología de Prevencion de Riesgos, en la que se describen un conjunto de pasos que se deben llevar a cabo anticipadamente para mitigar la proximidad de un daño y asi evitar el mal tratamiento de los datos personales, que puede colocar en riesgo la seguridad de un sistema de información académica. Esta metodología es una metodología fácil de entender y que se centra en el factor humano.

5.2.2 PROPÓSITO

Esta metodología proporciona una base para el desarrollo de un programa de prevención de riesgos eficaz, y contiene las definiciones y la orientaciones prácticas necesarias para identificar, evaluar y prevenir los riesgos encontrados en un sistema de información académica.

Además, esta metodología proporciona información para la selección de controles preventivos que ayuden al manejo adecuado de la información personal por parte de los usuarios de los sistemas de información académica.

5.2.3 OBJETIVO

El objetivo de esta metodología de prevención de riesgos es que las instituciones educativas puedan cumplir su misión: (1) previniendo el daño y mal manejo de los activos que hacen parte del sistema de información académica; (2) reduciendo los gastos debidos a la recuperación de los activos y (3) proporcionando documentación útil para el sistema de gestión de seguridad de la información (SGSI)

5.2.4 PÚBLICO OBJETIVO

Esta metodología esta dirigida al personal de Tecnologías de Información (TI) de las instituciones educativas y a los expertos en seguridad informática.

5.2.5 REFERENCIAS RELACIONADAS CON

Esta metodología está basada en diferentes metodologías de prevención y gestión de riesgos encontradas en la literatura (OCTAVE (Caralli, Stevens, Young, & Wilson, 2007), CORAS(SINTEF, 2006) , Metodología de Administración de Riesgos según Estándar Australiano (*AS/NZS 4360:1999 -Estándar Australiano, Administración de Riesgos*, 1999), NTC-ISO/IEC 27005: Gestión del Riesgo en la Seguridad de la Información (ICONTEC, 2009), CRAMM , MAGERIT(Villalba, 2002) , Metodología de Gestión de Riesgos para Sistemas de Tecnologías de la Información según NIST (NIST, 2001), Metodología para el Diagnóstico, Prevención y Control de la Corrupción en Programas de Seguridad Ciudadana según el BID (García Mejía, 2010) y Metodología de Prevención de Incidentes de Malware según NIST (Mell et al., 2005), así como en el modelo de defensa en profundidad (Álvarez Marañón & Pérez García, 2004) y el libro Implementación de un Sistema de Gestión de Seguridad de la Información según ISO 27001: Un Enfoque Práctico (Merino Bada & Cañizares Sales, 2011).

5.2.6 ESTRUCTURA DE LA METODOLOGÍA

La metodología está estructurada en 4 pasos:

- Paso1: Establecimiento del Contexto
- Paso 2: Identificación de Riesgos
- Paso 3: Análisis de Riesgos
- Paso 4: Prevención de Riesgos

5.2.7 PASO 1: ESTABLECIMIENTO DEL CONTEXTO

Consiste en identificar los activos importantes para el sistema de información académica, los requisitos de seguridad de esos activos, lo que la organización está haciendo para proteger dichos activos, y los objetivos que se persiguen con el análisis de riesgos. Para ello, se debe responder a las siguientes preguntas:

1. **¿Cuáles son los activos institucionales relacionados con el sistema de información académica?**

   Para responder a esta pregunta, se deben identificar primero los procesos que se llevan a cabo a través del sistema de información académica, como: consulta de datos personales de estudiantes y docentes (hoja de vida), consulta de información académica (materias, horarios, notas, etc.) de los estudiantes, registro de notas de los estudiantes por parte de los docentes, modificación de datos personales por parte de estudiantes y docentes, modificación de información académica, etc. A partir de la información obtenida, se deben identificar los activos involucrados en cada uno de los procesos. Estos activos pueden agruparse, según su naturaleza. A continuación se presenta una clasificación de los activos encontrados comúnmente en un sistema de información académica. Sin embargo, es posible que no todos estén presentes en el sistema o que haya otros activos que no se mencionan en esta clasificación.

   - **Activos de Información:** A esta categoría corresponderían los activos que contienen o transportan información de los usuarios del sistema de información académica. Dentro de esta categoría se tienen otros tipos de activos

     - **Hardware:** A esta subcategoría pertenecen los equipos y dispositivos utilizados por la institución y por los usuarios del sistema de información académica. Por ejemplo:

       - Servidores del sistema de información académica.
       - Dispositivos utilizados por los usuarios para acceder al sistema de información académica (Teléfonos Móviles, PCs, portátiles, etc.).

     - **Software:** A esta subcategoría pertenecen las aplicaciones que se utilizan para hacer uso del sistema de información académica. Por ejemplo:

       - Aplicación de autenticación para ingresar al sistema de información académica
       - Base de datos de información académica
       - Navegador WEB de los usuarios, utilizado para ingresar al sistema de información académica

        - **Red:** A esta subcategoría pertenece el canal de comunicación y los dispositivos de red (*switches*, *routers*, etc.) que utiliza la institución para que los usuarios puedan acceder al sistema de información académica. Por ejemplo:
            - Canal de comunicación cliente/servidor
            - *Router* Frontera
    - **Personal:** En esta categoría se ubican los diferentes grupos de usuarios del sistema de información académica. Por ejemplo:
        - Estudiantes
        - Docentes
        - Administrativos
        - Personal encargado del área de Tecnologías de la Información (TI)
    - **Sitio:** En esta categoría se encuentran los diferentes lugares en donde se ubican los equipos y dispositivos de la institución y del usuario (hardware). Por ejemplo:
        - Centro de datos donde están los servidores del sistema de información académica.
        - Lugar desde donde consultan los usuarios el sistema de información académica (café internet, domicilio, universidad).
    - **Organización:** A esta categoría pertenecen los aspectos que son responsabilidad y le interesan directamente a la institución. Por ejemplo:
        - Imagen y reputación de la institución.
        - Políticas del sistema de información académica.

2. **¿Qué funciones desempeña cada uno de los activos del sistema de informaciòn académica?**

   Una vez identificados los activos, es sencillo establecer qué función o funciones tiene cada uno dentro del sistema de información académica, según los procesos idenficados.

3. **¿Qué personas son responsables de la seguridad y la administración de los activos del sistema de información académica?**.

   Ahora, se determina quién o quiénes son los responsables de cada activo. Interesan especialmente los activos que son responsabilidad de la institución, pues algunos de los activos identificados son propiedad de los usuarios. Sin embargo, los activos que son responsabilidad del usuario deben tenerse en cuenta en el momento de realizar las campañas de concientización sobre el uso adecuado y seguro de los mismos.

4. **¿Qué información manejada en el sistema de información académica es confidencial y qué nivel de privacidad debe tener dicha información?**

   Primero, se debe identificar qué información personal está almacenada en el sistema de información académica como: datos personales de estudiantes y docentes, información profesional de estudiantes y docentes, información académica del estudiante (notas, materias, horarios), etc. Luego, se debe establecer qué grado de confidencialidad debe tener dicha información.

5. **¿Qué leyes de seguridad informática, a nivel nacional y regional, aplican al sistema de información académica?**

   Es importante conocer la normativa que regula el manejo de las bases de datos de información personal y de sistemas de información académica en el territorio donde opera el sistema de información académica. Estas darán las pautas a tener en cuenta para manejar de manera adecuada la información del sistema de información académica. Las leyes, a nivel colombiano, a tener en cuenta son: la Ley 1581 de 2012 (Protección de Datos Personales) y la ley 1273 de 2009 (Delitos Informáticos).

6. **¿Qué políticas de seguridad institucionales son aplicables a cada uno de los activos del sistema de información académica?**

   Para esto, se debe consultar el documento de las políticas de seguridad institucionales y centrarse en lo que dicen con respecto a los activos antes identificados.

7. **¿Qué expectativas tienen los diferentes usuarios del sistema de información académica con respecto a su funcionamiento y seguridad?**, y **¿Qué consecuencias negativas traería el defraudar dichas expectativas para el buen nombre y reputación de la institución?.**

   Aquí se deben tener en cuenta los diferentes grupos de personas que usan el sistema, como: administrativos, docentes, estudiantes, personal de TI, etc. Para conocer las expectativas de los usuarios y las consecuencias de defraudar dichas expectativas, se pueden realizar encuestas o entrevistas a una muestra representativa de cada grupo.

Además, se debe definir el alcance y amplitud de las actividades de análisis de riesgos que se van a llevar a cabo. De acuerdo al presupuesto y al tiempo con el que se disponga, el personal de TI puede decidir centrarse solo en los activos más importantes del sistema de información académica o realizar un análisis completo que incluya todos los activos. Ya que las personas son el eslabón más débil en la cadena de la seguridad (Lizarazo Rueda, 2012), se debe tratar de no concentrarse solamente en los activos de información sino también considerar los de personal.

5.2.8 PASO 2: IDENTIFICACIÓN DE RIESGOS

Consiste en determinar qué vulnerabilidades poseen los diferentes activos del sistema de información académica e identificar las amenazas que pueden explotarlas. Para ello se deben seguir los siguientes pasos:

1. **Valoración de los Activos:** Se debe determinar cuáles de los activos identificados son los más importantes para el sistema de información académica. Esta valoración puede hacerse considerando el impacto que tiene para el sistema de información académica y para la institución una pérdida en la confidencialidad, integridad y disponibilidad de cada activo. El resultado de esta valoraciòn es una lista con los activos priorizados, y los activos de mayor prioridad son los que serán sometidos a la gestión de riesgos. El número de activos seleccionados, dependerá del alcance especificado para el análisis de riesgos en el paso anterior.

   La valoración de estos activos puede ser (NIST, 2001):

   - *Cualitativa:* Se utilizan escalas descriptivas para indicar las concecuencias potenciales de una pérdida en la confidencialidad, integridad o disponiblidad del activo. Este tipo de valoración se usa como una actividad inicial para identificar los riesgos que requieren análisis más detallado, cuando el nivel de riesgo no justifica el tiempo y esfuerzo requerido para un análisis más completo o cuando los datos numéricos son inadecuados para un análisis cuantitativo.

   - *Semi-cuantitativa:* En esta valoración a las escalas cualitativas se les asignan valores, y el número asignado a cada descripción no tiene que guardar una relación precisa con la magnitud real de las consecuencias que trae una pérdida en la confidencialidad, integridad o disponiblidad del activo. El análisis semi-cuantitativo puede no diferenciar apropiadamente entre distintos riesgos, particularmente cuando las consecuencias son extremas.

   - *Cuantitativa*: Este tipo de valoración utiliza valores numéricos para las concecuencias de una pérdida en la confidencialidad, integridad o disponiblidad del activo en lugar de escalas descriptivas. Utiliza datos de distintas fuentes como: registros anteriores, experiencia relevante, prácticas y experiencia de la industria, literatura relevante publicada, investigaciones de mercado, experimentos y prototipos, modelos económicos, opiniones y juicios. La calidad de este análisis depende de la precisión e integridad de los valores numéricos utilizados.

Una escala muy utilizada para valorar los activos y determinar el impacto que tendría la pérdida de disponibilidad, integridad y confidencialidad de los mismos para la institución, es la escala de Likert. Esta escala es semi-cuantitativa. A continuaciòn se muestra un ejemplo de escala de Likert:

- 1: Muy bajo

- 2: Bajo
- 3: Medio
- 4: Alto
- 5: Muy alto

La Tabla 5 muestra las columnas que debería tener la Tabla de Valoración de Activos. Se debe dar un valor en la escala que se haya definido, para cada uno de los pilares de la seguridad informática (disponibilidad, integridad y confidencialidad) por cada activo, y luego colocar el promedio de los 3 valores en la columna Total. Cuando ya se hayan valorado todos los activos, estos deben ordenarse de mayor a menor valor y darles un orden de prioridad (los de mayor valor tendrán un menor número de prioridad). Si existen dos o más activos que tengan el mismo valor, el evaluador debe decidir, según su criterio, cuál de los activos es más importante para el sistema de información académica y de acuerdo a ello darle un valor de prioridad.

La valoración de los activos de personal no se puede hacer considerando la disponibilidad, integridad y confidencialidad, pues estas características son propias de los activos de información pero no de un ser humano. Por ello, se deben considerar otros indicadores, que fueron tomados de (Ramos Lara, 2014), donde se afirma que: "los indicadores operativos de los recursos humanos son: conocimientos, aptitudes y actitudes o habilidades de los empleados" . Para ello, se va a utilizar la siguiente escala de Likert. Por tanto, se debe considerar el impacto que tiene para el sistema de información académica el que las personas no cuenten con los conocimientos, aptitudes y actitudes necesarias para manejarlo. La Tabla 6 es un ejemplo de la tabla que se debe elaborar para valorar los activos de personal. Para realizar esta valoración se sigue el mismo procedimiento indicado anteriormente para los activos de información. Tenga en cuenta, que al priorizar los activos, se deben incluir tanto los activos de información como los activos de personal en la numeración.

Tabla 5. Ejemplo de Tabla para Valoración de Activos

Fuente: Diseño de un Sistema de Gestión de Seguridad de Información: Óptica ISO 27001:2005 (Alexander, 2007)

ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	TOTAL	ORDEN DE PRIORIDAD

Tabla 6. Ejemplo de Tabla para la Valoración de Activos de Personal

ACTIVOS	CONOCIMIENTOS	APTITUDES	ACTITUDES	TOTAL	ORDEN DE PRIORIDAD

- **Identificación de Vulnerabilidades:** Una vulnerabilidad es una falla o debilidad de un activo que puede propiciar una violación de la seguridad o de las políticas del sistema.

  Para determinar las vulnerabilidades que posee cada activo se debe recurrir a los responsables de dicho activo e indagar sobre las causas de los incidentes de seguridad que ha presentado dicho activo, lo que se ha hecho para evitar que se repitan esos incidentes y qué tan efectivas han sido las medidas tomadas. Además, se debe verificar que cada activo cuente con la seguridad especificada por los responsables del mismo, a través de una auditoría o, si se trata de software, a través de hacking ético, y elaborar una lista de comprobación de los requisitos de seguidad de dicho activo.

  También es importante determinar qué permisos o privilegios tienen los diferentes tipos de usuarios que acceden al sistema de información académica sobre cada activo y qué tan perjudicial puede resultar para el sistema el que dichos usuarios hagan mal uso de esos permisos. Además, se deben identificar, a través de la literatura, cuáles son las vulnerabilidades más comunes de cada activo.

- **Identificación de Amenazas:** Una amenaza es un evento que puede causar daño en los activos tales como la información, los procesos y los sistemas. Estas pueden ser de origen natural o humano, podrian ser acccidentales o deliberadas, y algunas de estas pueden afectar a más de un activo. En tales casos, pueden causar diferentes impactos, dependiendo de los activos que se vean involucrados. Los aspectos ambientales y culturales también se deben tener en cuenta cuando se consideran las amenazas. Se deben identificar las amenazas que pueden explotar las vulnerabilidades identificadas previamente y causar daños en los activos del sistema de información académica.

  Para determinar las amenazas que afectan a cada activo se debe recurrir a los responsables de dicho activo y obtener información sobre los incidentes que han afectado la disponiblidad o buen funcionamiento del mismo, así como la frecuencia con que cada incidente se ha presentado.

  Se debe elaborar una tabla, como se muestra en la Tabla 7, donde se listen las vulnerabilidades de cada activo y las amenazas que pueden explotar cada una de dichas vulnerabilidades.

Tabla 7: Ejemplo de determinación de Amenazas y Vulnerabilidades

ACTIVOS	VULNERABILIDADES	AMENAZAS

5.2.9 PASO 3: ANÁLISIS DE RIESGOS

Consiste en calcular la probabilidad que una amenaza explote una determinada vulnerabilidad y establecer el nivel de riesgo de cada activo, priorizándolos para tomar acciones posteriormente.

Comunmente, los riesgos tienen dos factores: el primero expresa el impacto que ese riesgo tendría en el sistema y la organización si se presentara, y el segundo expresa la probabilidad de que ese riesgo ocurra. Los diferentes niveles de estos factores se pueden expresar a través de una escala de Likert, donde 1 represente el nivel más bajo y 5 el nivel más alto.

Para determinar el impacto del riesgo se deben tener en cuenta criterios como: (1) impacto económico, (2) tiempo de recuperación tras el incidente, (3) actividades o procesos de la institución que se verían afectados por dicho riesgo, (4) daño causado a la imagen de la institución.

Para determinar la probabilidad de ocurrencia, son importantes los datos proporcionados en el paso anterior por los responsables de los activos sobre la frecuencia con la que se ha presentado cada incidente de seguridad. Además, también se pueden tener en cuenta estadísticas presentadas por fuentes reconocidas en el área de seguridad, acerca de la frecuencia de los ataques que no se han presentado aún en el sistema de información académica pero que, de acuerdo a las vulnerabilidades encontradas, podrían ocurrir. Es recomendable calcular la probabilidad de ocurrencia de un incidente con base en los datos obtenidos en el último año. Si no se cuenta con dichos datos, se debe recurrir a las estadísticas de fuentes reconocidas en el área de la seguridad.

Para determinar el valor de la probabilidad de ocurrencia de los riesgos, es conveniente no utilizar una escala lineal sino exponencial, cuando se habla de la frecuencia con que ocurren los ataques. Por ejemplo, la escala de Likert presentada a continuación es una escala cuasi-exponencial, en la que se consideró con un nivel alto de riesgo el que un ataque ocurra el 50% de las veces.

- **0 – 4.99% :** 1 Muy Bajo.
- **5 – 14.99%:** 2 Bajo.
- **15 – 29.99%:** 3 Medio.
- **30 – 49.99 %:** 4 Alto.
- **50 – 100 %:** 5 Muy Alto

Luego de definir los rangos se procede a llenar la Tabla 8. Posteriormente, se debe calcular el riesgo, para lo cual, basta con multiplicar el impacto de la amenaza por la probabilidad de ocurrencia.

Finalmente, se realiza un priorización de los riesgos, ordenando los valores obtenidos del mayor al menor, dándole un número menor de prioridad a los riesgos de mayor valor. Se debe entonces establecer una escala en la que se determine el nivel del riesgo, como el ejemplo que se muestra a continuación, diferenciando por colores los niveles de riesgo.

- **1 – 4:** **Muy Bajo**

- **5 – 9:** **Bajo**
- **10 – 14:** **Medio**
- **15 – 19:** **Alto**
- **20 – 25:** **Muy Alto**

El resultado de esta valoración es un listado de los riesgos priorizados y diferenciados por su color.

Tabla 8: Ejemplo de Tabla de Valoración de Riesgo
Fuente: Diseño de un Sistema de Gestión de Seguridad de Información: Óptica ISO 27001:2005 (Alexander, 2007)

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN

5.2.10 PASO 4: PREVENCIÓN DE RIESGOS

El tratamiento de riesgos consiste en implantar contramedidas que permitan evitar, mitigar, aceptar o transferir los riesgos. Como esta es una metodología de prevención de riesgos, los controles que se van a implantar tienen como fin evitar que ocurran los riesgos.

Tenga en cuenta que la prevención de riesgos es un proceso continuo que consiste en analizar los riesgos existentes en un sistema de información, planear y ejecutar actividades, a corto y largo plazo, tendientes a evitar o reducir esos riesgos identificados, evaluar la efectividad de dichas actividades y actualizarlas, de acuerdo a los cambios en el entorno interno y externo de la organización.

Teniendo en cuenta la priorización de los riesgos realizada en el paso anterior, se deben implantar controles preventivos que ayuden a mitigar y prevenir los riesgos, principalmente los de mayor nivel.

Los elementos más importantes a tener en cuenta para plantear estrategias de prevenciòn de riesgos y los controles que se pueden llevar a cabo en cada uno de ellos, según son:

1. **Políticas**: Las instituciones deben asegurarse que sus políticas aborden: la sensibilización del personal y, la mitigación de amenazas y vulnerabilidades. A continuación se describen las actividades que se pueden llevar a cabo para prevenir los riesgos originados por la falta de políticas:

    1. **Definición de Políticas de Seguridad**: Estas políticas definen los lineamientos a seguir para preservar la seguridad de los activos del sistema de información académica.

       Producto: Políticas de Seguridad del Sistema de Información Académica.

Controles a Corto Plazo:

Tabla 9. Definición de Políticas de Seguridad: Controles a Corto Plazo

VULNERABILIDAD	CONTROLES
Falta de políticas de seguridad para el sistema de información académica	• Especificar los activos importantes para el sistema de información académica. • Asignar responsabilidades sobre cada activo a los diferentes cargos y usuarios. • Definir el nivel de seguridad que debe tener cada activo del sistema de información académica. • Clasificar la información manejada dentro del sistema de información académica (nivel de confidencialidad). • Especificar el manejo que se debe dar a cada activo del sistema de información académica según su nivel de seguridad • Especificar las sanciones a aplicar cada vez que se presente un incidente de seguridad determinado. • Determinar si las políticas de seguridad establecidas van en concordancia con las leyes de protección de datos personales y de seguridad informática vigentes a nivel nacional. Si no es así, realizar los ajustes necesarios. • Determinar si las políticas de seguridad establecidas van en concordancia con las políticas de seguridad institucionales. Si no es así, realizar los ajustes necesarios. • Obtener la aprobación de las políticas del sistema de información académica por parte de las directivas de la institución
Ausencia o insuficiencia en las disposiciones, con respecto a la seguridad de la información, en los contratos de los empleados	• Establecer los términos y condiciones legales de contratación relacionados con la confidencialidad y seguridad de la información gestionada en cada cargo.
Ausencia de asignación adecuada de	• Definir dentro de las funciones de los

VULNERABILIDAD	CONTROLES
responsabilidades, con respecto a la seguridad de la información, en la descripción de los cargos	cargos, quién se encargará de la seguridad de cada uno de los activos del sistema de información académica y las responsabilidades que tiene con dicho activo, como las sanciones en que incurriría si no lo trata adecuadamente. • Verificar que estas responsabilidades se especifiquen claramente en su contrato.
Ausencia de auditorías (supervisiones) regulares del sistema de información académica y los empleados	• Establecer los objetivos, alcance, criterios y frecuencia de las auditorías que se deben realizar a los activos del sistema de información académica y al personal a cargo de los mismos (ver Falta de programa de auditorías del sistema de información académica).
Ausencia de procedimientos de identificación y valoración de riesgos	• Elaborar procedimientos de identificación, valoración y análisis de riesgos.
Ausencia de procedimiento formal para el control de la documentación del SGSI	• Definir un procedimiento formal para el control de la documentación del SGSI
Ausencia de procedimiento formal para el retiro de usuarios del sistema y revisión periódica (supervisión) de los derechos de acceso, así como la asignación de dicha responsabilidad a un cargo específico	• Establecer los procedimientos de asignación y retiro de privilegios de acceso al sistema de información académica, de los diferentes tipos de usuarios. • Definir procedimientos formales para la revisión periódica (supervisión) de los derechos de acceso al sistema de información académica de cada usuario.
Falta de personal suficiente y sobrecarga de trabajo	• Definir correctamente los perfiles de las personas a contratar, en cuanto a conocimientos y cualidades humanas que deben tener. • Realizar la selección, contratación y capacitación de personal en las áreas con sobrecarga de trabajo
Procedimientos inadecuados de contratación	• Redefinir los pasos que se deben llevar a cabo para la contratación del personal • Definir correctamente los perfiles de

VULNERABILIDAD	CONTROLES
	las personas a contratar, en cuanto a conocimientos y cualidades humanas que deben tener.
Corrupción	• Realizar auditorías periódicas a los empleados y su trabajo (ver Falta de programa de auditorías del sistema de información académica) • Aplicar sanciones establecidas a las personas que no hacen correctamente su trabajo

Controles a Largo Plazo:

Tabla 10. Definición de Políticas de Seguridad: Controles a Largo Plazo

VULNERABILIDAD	CONTROLES
Falta de políticas de seguridad del sistema de información académica	• Realizar revisiones periódicas de las políticas de seguridad del sistema de información académica, de manera que sean adecuadas para el contexto interno como externo de la institución
Ausencia de auditorías (supervisiones) regulares del sistema de información académica y los empleados	• Realizar auditorías periódicas del sistema de información académica como de los empleados y su trabajo (ver Falta de programa de auditorías del sistema de información académica)
Ausencia de procedimientos de identificación y valoración de riesgos	• Ejecutar los procedimientos de identificación, valoración y análisis de riesgos para identificar los riesgos todavía presentes en el sistema.
Ausencia de procedimiento formal para el control de la documentación del SGSI	• Aplicar el procedimiento establecido y documentar adecuadamente el SGSI
Ausencia de procedimiento formal para el retiro de usuarios del sistema y revisión periódica (supervisión) de los derechos de acceso, así la asignación de dicha responsabilidad a un cargo específico	• Revisar periódicamente los derechos de acceso al sistema de información académica de cada usuario.
Falta de personal suficiente y sobrecarga de trabajo	• Revisar las funciones de cada cargo y determinar si estas funciones deben ser redistribuidas de manera más equitativa para evitar sobrecargas • Realizar los cambios pertinentes en la definición de funciones de los cargos

VULNERABILIDAD	CONTROLES
Procedimientos inadecuados de contratación	• Realizar las entrevistas y las pruebas necesarias para verificar que los candidatos cumplen con los perfiles establecidos • Capacitar adecuadamente al nuevo personal antes de que empiece a desempeñar su cargo
Corrupción	• Realizar jornadas de concientización a los empleados, indicando las sanciones que trae el hacer mal uso de los activos del sistema de información académica (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)

Actores Principales: Personal de TI, Directivas de la Institución

2. **Concientización:** Se debe crear un programa de sensibilización efectivo que explique el uso adecuado de los activos del sistema de información académica. A continuación se describen las actividades que se pueden llevar a cabo para prevenir los riesgos originados por la falta de concientización:

    1. **Definición de Programas de Concientización:** Estos programas buscan que los diferentes grupos de usuarios manejen adecuadamente los activos y la información del sistema de información académica. Se debe definir un programa diferente por cada grupo de usuarios, ya que dependiendo del rol y los privilegios de estos usuarios en el sistema de información académica, va a cambiar el grado de profundidad y especialización de cada programa.

        Producto: Programas de Concientización: de los Estudiantes, de los Profesores, de los Administrativos y del Personal de TI.

        Controles a Corto Plazo:

Tabla 11. Definición de Programas de Concientización: Controles a Corto Plazo

VULNERABILIDAD	CONTROLES
Falta de capacitación y concientización en seguridad	• Identificar los errores comunes que comete el grupo de usuarios objetivo de cada programa al manejar el sistema de información académica, y que colocan en riesgo la información almacenada en él. • Definir los objetivos del programa de concientización • Establecer la estructura del programa

VULNERABILIDAD	CONTROLES
	de concientización, definiendo las diferentes fases que lo conformarán. Se debe tener en cuenta que dicha concientización debe realizarse desde el momento en que la persona entra a hacer parte de la institución y luego realizar periódicamente actividades que refuercen y actualicen lo aprendido. • Obtener la aprobación y financiamiento del programa por parte de las directivas de la institución • Seleccionar los temas que se van a abordar durante la concientización. Entre los temas a tener en cuenta están: leyes de delitos informáticos y de protección de datos personales, importancia del rol de cada tipo de usuario en la cadena de seguridad, precauciones que se deben tener antes de acceder al sistema de información acádemica, medidas de seguridad que se deben tener en cuenta mientras se esté consultando el sistema, medidas de seguridad que se deben tener con la información que se descarga o sube al sistema, características mínimas que debe tener la contraseña de acceso al sistema de información académica para que sea segura. • Definir las estrategias y actividades a llevar a cabo para desarrollar los diferentes temas del programa • Elaborar el material que se utilizará en las actividades de concientización • Entrenar al personal que se encargará de realizar la concientización
Percepción errónea de la seguridad del sistema por parte de los usuarios	• Explicar adecuamente a los usuarios, desde la primera vez que ingresen al sistema, cómo funcionan las medidas de seguridad implantadas y qué rol juegan ellos en la cadena de la

VULNERABILIDAD	CONTROLES
	seguridad.

Controles a Largo Plazo:

Tabla 12. Definición de Programas de Concientización: Controles a Largo Plazo

VULNERABILIDAD	CONTROLES
Falta de capacitación y concientización en seguridad	• Realizar las actividades de concientización planteadas • Entregar el material elaborado para las diferentes actividades (posters, boletines, etc.) • Monitorear el programa de concientización • Documentar y evaluar los resultados del programa de concientización • Realizar los cambios que se crean pertinentes al programa de concientización

Actores Principales: Directivas de la Institución, Personas Encargadas de la Concientización, Estudiantes, Profesores, Administrativos y Personal de TI

2. **Difusión de las Políticas de Seguridad:** Esta difusión busca que los diferentes grupos de usuarios conozcan las políticas de seguridad existentes sobre el manejo adecuado de los activos y la información del sistema de información académica, sus responsablidades y las sanciones que se aplicarían en caso de incumplimiento. La difusión de estas políticas debe hacerse en el momento en que cada persona entra a ser parte de la institución.

   Producto: Estrategias de Difusión de Políticas de Seguridad a los Estudiantes, Profesores, Administrativos y Personal de TI.

   Controles a Corto Plazo:

Tabla 13. Difusión de las Políticas de Seguridad: Controles a Corto Plazo

VULNERABILIDAD	CONTROLES
Desconocimiento de las políticas de seguridad del sistema de información académica por falta de divulgación	• Asignar la responsabilidad de la creación e implementación de las estrategias de difusión a un cargo o área específica. • Establecer qué políticas de seguridad aplican a cada grupo de usuarios. • Definir la estrategia de difusión de las políticas de seguridad a cada grupo de usuarios.

VULNERABILIDAD	CONTROLES
	• Obtener la aprobación y financiamiento de las estrategias de difusión por parte de las directivas de la institución • Elaborar el material que se utilizará para difundir las políticas

Controles a Largo Plazo:

Tabla 14. Difusión de las Políticas de Seguridad: Controles a Largo Plazo

VULNERABILIDAD	CONTROLES
Desconocimiento de las políticas de seguridad del sistema de información académica por falta de divulgación	• Dar a conocer las políticas de seguridad a cada grupo de usuarios • Monitorear las estrategias de difusión • Documentar y evaluar los resultados de las estrategias de difusión • Realizar los cambios que se crean pertinentes en las estrategias de difusión

Actores Principales: Directivas de la Institución, Personas Encargadas de Difundir las Políticas, Estudiantes, Profesores, Administrativos y Personal de TI

3. **Mitigación de Vulnerabilidades y Amenazas:** Mitigar vulnerabilidades es muy importante para la prevención, especialmente cuando dichas vulnerabilidades son conocidas públicamente. Por otra parte, la mitigación de amenazas se debe realizar para detectar y detener a los atacantes antes de que afecten al sistema de información académica. A continuación se describen las actividades que se pueden llevar a cabo para prevenir los riesgos originados por las vulnerabilidades y amenazas:

    1. **Coordinación de la Seguridad del Sistema de Información Académica:** Esta coordinación busca que todas las actividades tendientes al manejo de la seguridad de los diferentes activos y la documentación del SGSI se realicen de manera ordenada, y cumplan con las políticas de seguridad establecidas.

        Producto: Documentación del SGSI, Reportes de Incidentes de Seguridad, Procedimientos y Planes de Acción del SGSI, Reportes de Auditorías.

        Controles a Corto Plazo:

Tabla 15. Coordinación de la Seguridad del Sistema de Información: Controles a Corto Plazo

VULNERABILIDAD	CONTROLES
Falta de medidas de seguridad en los activos del sistema de información académica	• Especificar las medidas de seguridad que se deben implantar en cada activo del sistema de información académica • Comprometer a los directivos de la institución para que apoyen las diferentes actividades de implantación de las medidas de seguridad del sistema de información académica
Falta de procedimientos formales de manejo de incidentes de seguridad	• Establecer el procedimiento que se debe seguir para reportar los incidentes de seguridad de los activos del sistema de información académica • Definir los planes de acción que se llevarán a cabo cuando se presenten incidentes de seguridad y el tiempo máximo de respuesta a cada incidente. • Establecer la forma en que se deben documentar los incidentes de seguridad
Falta de programa de auditorías del sistema de información académica	• Especificar de manera detallada el programa de auditoría que se debe llevar a cabo para supervisar los activos del sistema de información académica como el personal a cargo de los mismos • Asignar las responsabilidades al equipo auditor. • Entrenar al equipo auditor • Establecer el calendario de las auditorías

Controles a Largo Plazo:

Tabla 16. Coordinación de la Seguridad del Sistema de Información: Controles a Largo Plazo

VULNERABILIDAD	CONTROLES
Falta de medidas de seguridad en los activos del sistema de información académica	• Implantar las medidas de seguridad en cada activo del sistema de información académica.
Falta de procedimientos formales de manejo de incidentes de seguridad	• Reportar los incidentes de seguridad que se presenten en los activos del sistema

VULNERABILIDAD	CONTROLES
	• Realizar actividades de recuperación ante incidentes • Documentar los incidentes de seguridad • Analizar los incidentes de seguridad y determinar estadísticamente su probabilidad de ocurrencia • Realizar los cambios pertinentes en la ubicación, configuración y medidas de seguridad de cada activo para evitar incidentes futuros
Falta de programa de auditorías del sistema de información académica	• Implementar el programa de auditoría. • Documentar las actividades de auditoría • Analizar la información obtenida en las actividades de auditoría, identificando las vulnerabilidades aún presentes en cada uno de los activos • Evaluar la conformidad del programa de auditoría con el calendario y los objetivos establecidos • Evaluar el desempeño de los miembros del equipo auditor. • Realizar los ajustes necesarios en el programa de auditoría y los cambios pertinentes en el equipo auditor.

Actores Principales: Personal de TI, Directivas de la Institución, Equipo Auditor

2. **Seguridad Física:** Esta busca proteger los lugares donde se encuentran los activos del sistema de información académica.

   Producto: Medidas de Seguridad Física

   Controles a Corto Plazo:

Tabla 17. Seguridad Física: Controles a Corto Plazo

VULNERABILIDAD	CONTROLES
Ubicación en un área susceptible a inundación y desastres naturales	• Ubicar los equipos en un área que no sea susceptible a desastres naturales
Sensibilidad a la radiación electromagnética	• Ubicar los equipos en un lugar donde no ocurran radiaciones electromagnéticas fuertes
Falta de aire acondicionado	• Colocar aire acondicionado en el

VULNERABILIDAD	CONTROLES
	lugar donde se encuentran los equipos
Susceptibilidad a humedad, polvo y suciedad.	• Verificar que el lugar donde se encuentran los equipos no tiene filtraciones o algún tipo de humedad que pueda afectarlos
Red eléctrica inestable	• Verificar que la instalación eléctrica del lugar donde se encuentran los equipos cuenta con la suficiente potencia y está en óptimas condiciones para soportarlos todos • Conectar los equipos a través de un regulador a la red eléctrica • Adquirir UPSs para los equipos, a fin que no salgan de funcionamiento cuando hayan cortes de energía
Falta de plan de contingencia	• Elaborar plan de contingencia para el lugar donde se encuentran los equipos, a fin de saber cómo actuar ante incidentes o fallas inesperados
Falta de control de acceso al lugar donde se encuentran los equipos	• Colocar rejas de seguridad en las ventanas • Ubicar los equipos de manera que no queden cerca a las ventanas • Controlar el acceso al lugar donde se encuentran los equipos, de manera que sólo personas autorizadas puedan acceder a él
Falta de control de acceso y seguridad física en los sitios donde se consulta el sistema de información académica	• Tomar precauciones de seguridad al ingresar al sistema, para no exponer la contraseña de acceso y evitar fisgones. • No olvidar cerrar la sesión del sistema de información académica. • Borrar rastros de navegación del computador antes de irse

Controles a Largo Plazo:

Tabla 18.Seguridad Física: Controles a Largo Plazo

VULNERABILIDAD	CONTROLES
Falta de aire acondicionado	• Realizar mantenimiento periódico al aire acondicionado
Susceptibilidad a humedad, polvo y suciedad.	• Realizar con frecuencia una limpieza adecuada del lugar donde se

VULNERABILIDAD	CONTROLES
	encuentran los equipos
Red eléctrica inestable	• Realizar mantenimiento periódico a la instalación eléctrica del lugar donde se encuentran los equipos
Falta de plan de contingencia	• Revisar el plan de contingencia periódicamente para realizar mejoras • Dar a conocer el plan de contingencia al personal de TI encargado del lugar donde se encuentran los equipos
Falta de control de acceso al lugar donde se encuentran los equipos	• Verificar la efectividad de cada una de las medidas de seguridad física implementadas y realizar los cambios que se consideren necesarios • Instalar un sistema de videovigilancia para visualizar quienes ingresan al lugar donde se encuentran los equipos
Falta de control de acceso y seguridad física en los sitios donde se consulta el sistema de información académica	• Buscar un sitio que brinde mejores condiciones de seguridad para ingresar al sistema de información académica

Actores Principales: Personal de TI, personal de mantenimiento y limpieza, Docentes, Estudiantes, Administrativos.

3. **Defensa del Perímetro:** Esta busca proteger el lugar donde la red interna de la institución entra en contacto con la red externa

   Producto: Medidas de Seguridad del Perímetro

   Controles a Corto Plazo:

Tabla 19. Defensa del Perímetro: Controles a Corto Plazo

VULNERABILIDAD	CONTROLES
Conexiones a red pública sin protección	• Instalar un *firewall* en el perímetro de la red • Determinar las reglas que se deben configurar para controlar el tráfico entrante y saliente de la red institucional • Configurar correctamente en el *firewall*, las reglas de control de tráfico establecidas • Instalar y configurar un sistema de detección de intrusos (IDS) integrado

VULNERABILIDAD	CONTROLES
	con el *firewall*. • Instalar y configurar un servidor SNMP que permita monitorear el enlace con el ISP (Proveedor de Servicios de Internet) y el *firewall*.

Controles a Largo Plazo:

Tabla 20.Defensa del Perímetro: Controles a Largo Plazo

VULNERABILIDAD	CONTROLES
Conexiones a red pública sin protección	• Monitorear constantemente el tráfico del enlace con el ISP y el *firewall*. • Revisar constantemente los logs (bitácoras) del servidor SNMP • Analizar la información entregada por el servidor SNMP y sacar estadísticas • Verificar periódicamente la efectividad del *firewall* y del IDS • Realizar los cambios en la configuración del *firewall*, del IDS y del servidor SNMP que se consideren necesarios.

Actores Principales: Personal de TI

4. **Defensa de la Red:** Esta busca proteger la información mientras viaja por la red

   Producto: Medidas de Seguridad de la Red

   Controles a Corto Plazo:

Tabla 21. Defensa de la Red: Controles a Corto Plazo

VULNERABILIDAD	CONTROLES
Información viajando en claro por la red Usuario y contraseña viajando en claro por la red	• Cifrar la información mientras viaja por la red, a través de algún protocolo seguro, como SSL/TLS.
Gestión inadecuada de la red	• Contratar el ancho de banda necesario para el sistema de información académica, según el volumen de tráfico que este maneja. • Hacer los cambios necesarios en la topología física de la red para que se

VULNERABILIDAD	CONTROLES
	aisle adecuadamente el tráfico del sistema de información académica del resto de la red, que este tráfico pase por enlaces de alta velocidad y que no hayan en el trayecto dispositivos que ocasionen cuellos de botella.

Controles a Largo Plazo:

Tabla 22. Defensa de la Red: Controles a Largo Plazo

VULNERABILIDAD	CONTROLES
Gestión inadecuada de la red	• Monitorear constantemente los servidores, los dispositivos de red y los enlaces por donde se enruta el tráfico del sistema de información académica, a través de un servidor SNMP. • Analizar la información entregada por el servidor SNMP y sacar estadísticas. • Realizar los cambios que se consideren necesarios en los servidores y en la red para solucionar los problemas que se presentan.

Actores Principales: Personal de TI

5. **Defensa de los Equipos:** Esta busca proteger los equipos relacionados con el sistema de información académica

Producto: Medidas de Seguridad de los Equipos

Controles a Corto Plazo:

Tabla 23. Defensa de los Equipos: Controles a Corto Plazo

VULNERABILIDAD	CONTROLES
Ausencia de esquemas de reemplazo periódico	• Planear el reemplazo periódico de los equipos.
Acceso de múltiples personas y uso compartido del equipo	• Crear cuentas de usuario en el equipo, de administrador y usuarios estándar. Nota: Se debe limitar el número de personas con permisos de acceso a los servidores al mínimo. • Realizar jornadas de concientización y capacitación a los usuarios del

VULNERABILIDAD	CONTROLES
	sistema de información académica sobre las medidas de seguridad a tener en cuenta en los equipos (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Falta de contraseña robusta de administrador	• Configurar contraseñas seguras para cada una de las cuentas de usuario. Se recomienda que la contraseña de la cuenta de administrador sólo la conozca una sola persona.
Ausencia de terminación de sesión cuando se abandona el equipo	• Configurar el equipo para que se bloquee automáticamente mínimo después de un minuto de inactividad y que solicite la contraseña para desbloquearse. • Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre las medidas de seguridad a tener en cuenta en los equipos (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Falta de puntos de restauración del sistema	• Insertar puntos de restauración en el sistema cada vez que se realicen cambios en la instalación o configuración del equipo
Copia no controlada de la información del servidor	• Almacenar las copias de respaldo de la información en un lugar seguro y de manera ordenada • Limitar el número de personas con permisos de acceso al servidor y sus copias de respaldo
Ausencia de revisión periódica de las bitácoras (logs) del servidor y de monitoreo del sistema en busca de fallas e incidentes de seguridad	• Revisar diariamente los logs (bitácoras) del servidor, para detectar posibles fallos que se estén presentando.
Susceptibilidad a las variaciones de voltaje (falta de regulador y UPS)	• Conectar el equipo a la red eléctrica a través de un regulador
Descarga descontrolada e instalación de software libre	• Crear cuentas de usuario en el equipo, de manera que exista un solo administrador, quien será el único con permisos para instalar programas. Para conectarse a

VULNERABILIDAD	CONTROLES
	Internet, deberán usarse las cuentas de usuario estándar o de invitado, nunca la cuenta de administrador. • Instalar un buen antivirus en el equipo • Actualizar diariamente el antivirus • Instalar y configurar adecuadamente un *firewall* de aplicación en el equipo • Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre las medidas de seguridad a tener en cuenta en los equipos (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Mantenimiento insuficiente	• Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre las medidas de seguridad a tener en cuenta en los equipos (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Falta de condiciones de refrigeración adecuadas	• Revisar si los ventiladores del equipo están funcionando adecuadamente, y si no es así, realizar la limpieza de los mismos o ver si se trata de un error en la conexión.

Controles a Largo Plazo:

Tabla 24. Defensa de los Equipos: Controles a Largo Plazo

VULNERABILIDAD	CONTROLES
Ausencia de esquemas de reemplazo periódico	• Realizar el reemplazo de los equipos según el esquema de reemplazo periódico
Falta de puntos de restauración del sistema	• Restaurar el sistema en caso de algún daño en el sistema operativo
Mantenimiento insuficiente	• Realizar periódicamente mantenimiento de software y hardware al equipo
Falta de control de los cambios hechos en la configuración del servidor	• Documentar adecuadamente los cambios en la configuración que se le realicen al servidor

VULNERABILIDAD	CONTROLES
Falta de contraseña robusta de administrador	• Cambiar periódicamente la contraseña de administrador por una contraseña que cumpla las características mínimas de seguridad
Susceptibilidad a las variaciones de voltaje (falta de regulador y UPS)	• Colocar UPS para que el equipo no salga de funcionamiento cuando se vaya la energía
Falta de condiciones de refrigeración adecuadas	• Colocar aire acondicionado en el sitio donde se encuentra el equipo

Actores Principales: Personal de TI, Docentes, Estudiantes, Administrativos

6. **Defensa de las Aplicaciones:** Esta busca proteger las aplicaciones relacionadas con el sistema de información académica

   Producto: Medidas de Seguridad de las Aplicaciones

   Control a Corto Plazo:

Tabla 25. Defensa de las Aplicaciones: Controles a Corto Plazo

VULNERABILIDAD	CONTROLES
Falta de mecanismo de autenticación fuerte, falta de complejidad de las contraseñas, y ausencia de límite de intentos de autenticación	• Si se utiliza autenticación usuario/contraseña, habilitar las directivas de las contraseñas para que se emplee un conjunto amplio de caracteres (mayúsculas, minúsculas, números, símbolos), que la contraseña tenga un número mínimo de caracteres, que haya un historial de contraseñas, que se deba cambiar la contraseña después de un número determinado de días y que se bloqueen las cuentas después de un número determinado de intentos fallidos.
Ausencia de terminación de sesión cuando se abandona la estación de trabajo	• Configurar los servicios para que las sesiones de los usuarios se terminen después de varios minutos de inactividad • Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre las medidas de seguridad a tener en cuenta en los equipos (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en

VULNERABILIDAD	CONTROLES
	Seguridad)
Copia no controlada de la información del servidor	• Asegurarse que solo tengan acceso a las copias de respaldo del servidor un reducido número de personas autorizadas.
Falta de confidencialidad de la contraseña de acceso al sistema de información académica Falta de precauciones de seguridad al ingresar al sistema de información académica Falta de configuración del navegador en cuanto a: bloqueo de cookies, almacenamiento de contraseñas, nivel de seguridad, almacenamiento de historial, etc. Instalación y activación indiscriminada de complementos	• Realizar jornadas de concientización y capacitación a los usuarios sobre el uso adecuado del sistema de información académica (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Especificaciones incompletas o no claras para los desarrolladores	• Si el sistema es propietario, elaborar o completar la documentación del software, de manera que sea comprensible para los desarrolladores
Fallas en el diseño e implementación del software que crean agujeros de seguridad	• Informar a los desarrolladores sobre las fallas encontradas
Interfaz de usuario compleja	• Capacitar a los usuarios sobre el uso adecuado de la aplicación y de las ayudas que posee

Controles a Largo Plazo:

Tabla 26. Defensa de las Aplicaciones: Controles a Largo Plazo

VULNERABILIDAD	CONTROLES
Falta de mecanismo de autenticación fuerte, falta de complejidad de las contraseñas, y ausencia de límite de intentos de autenticación	• Implementar un mecanismo de autenticación fuerte para ingresar al sistema de información académica, que involucre al menos dos factores (algo que se conoce, algo que se posee, algo que se es). • Monitorear el mecanismo de autenticación • Analizar los datos arrojados por el

VULNERABILIDAD	CONTROLES
	monitoreo del mecanismo de autenticación, a fin de determinar su efectividad
Fallas en el diseño e implementación del software que crean agujeros de seguridad Especificaciones incompletas o no claras para los desarrolladores	• Si el sistema de información académica es propietario, cuando se le vaya a hacer alguna modificación a las aplicaciones se debe usar una metodología de diseño de software que tenga en cuenta la seguridad y que posibilite realizar una buena documentación de los cambios realizados. • Si el sistema de información académica no es propietario, se deben reportar las fallas al creador del software
Defectos en el software e insuficiencia de pruebas del mismo	• Si el sistema de información académica es propietario, realizar pruebas al software, tras hacer modificaciones, antes de colocarlo a disposición de los usuarios • Si el sistema de información académica no es propietario, se deben reportar los defectos al creador del software
Interfaz de usuario compleja	• Si el sistema de información académica es propietario, elaborar un manual de usuario de la aplicación más específico, preguntar a los usuarios sobre las dificultades que encuentran en el uso de la interfaz y realizar los cambios necesarios a fin de reducir su complejidad • Si el sistema de información académica no es propietario, informar de las dificultades presentadas en su manejo a los desarrolladores

Actores Principales: Personal de TI, Docentes, Estudiantes, Administrativos

7. **Defensa de los Datos:** Esta busca proteger los datos almacenados en los equipos relacionados con el sistema de información académica

Producto: Medidas de Seguridad de los Datos

Controles a Corto Plazo:

Tabla 27. Defensa de los Datos: Controles a Corto Plazo

VULNERABILIDAD	CONTROLES
Almacenamiento sin la debida protección de la información académica	• Tener copias de respaldo de la información • Guardar la información de manera cifrada • Mantener vigilado el medio de almacenamiento de la información, para que no caiga en manos indeseadas
Falta de copias de respaldo	• Realizar diariamente copias de respaldo de la información importante
Falta de confidencialidad de la información que descarga del sistema de información académica	• Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre la seguridad que debe darse a la información que consultan y descargan del sistema (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad) • Guardar la información de manera cifrada • Mantener vigilado el medio de almacenamiento de la información, para que no caiga en manos indeseadas
Almacenamiento en claro de las contraseñas (tablas de contraseñas sin protección)	• Guardar las contraseñas de los usuarios de manera cifrada en la base de datos y los equipos
Ingreso de dispositivos de almacenamiento en equipos no protegidos Descuido del lugar donde se dejan los dispositivos de almacenamiento Ausencia de copias de respaldo de dispositivos de almacenamiento	• Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre la seguridad que debe darse a la información que consultan y descargan del sistema ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)

Controles a Largo Plazo:

Tabla 28. Defensa de los Datos: Controles a Largo Plazo

VULNERABILIDAD	CONTROLES

VULNERABILIDAD	CONTROLES
Almacenamiento sin la debida protección de la información académica	• Verificar la integridad de la información almacenada cuando sea necesario • Utilizar las copias de respaldo para recuperar la información en caso de algún daño
Falta de copias de respaldo	• Utilizar las copias de respaldo para recuperar la información en caso de algún daño

Actores Principales: Personal de TI, Docentes, Estudiantes, Administrativos

5.2.11 DIAGRAMA DE LA METODOLOGÍA

En la Figura 12 se muestran de manera resumida los pasos de la metodología MePRiSIA. Se debe tener en cuenta que una vez instauradas la medidas de prevención estas se deben revisar periódicamente para determinar si no están cumpliendo con su función o si han surgido nuevas amenazas, lo que implicaría volver a llevar a cabo los cuatro pasos de la metodología.

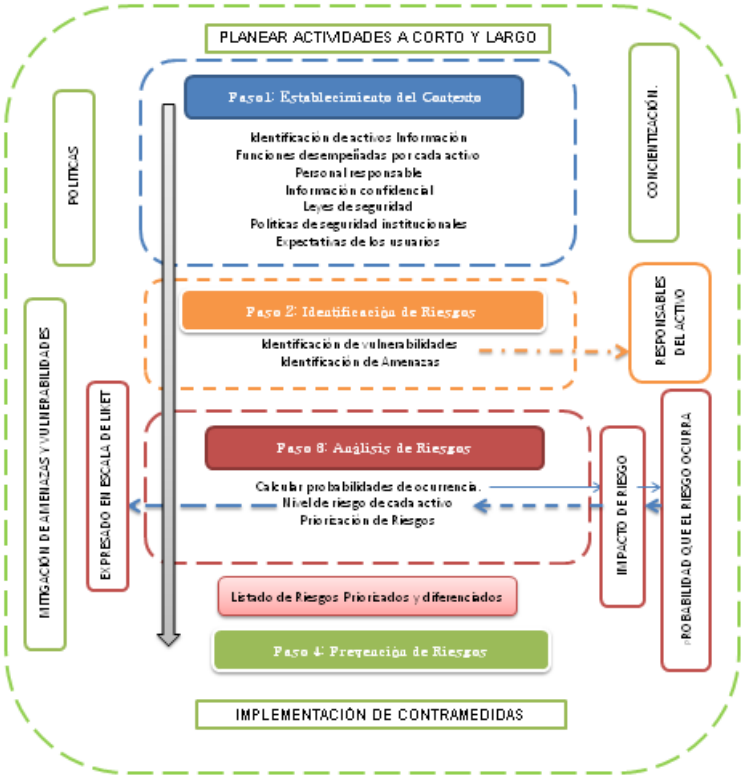

Figura 12. Diagrama de MePRiSIA

6 APLICACIÓN DE MEPRISIA AL SISTEMA DE INFORMACIÓN ACADÉMICA DE LA UNIVERSIDAD DE PAMPLONA

6.1 PASO 1: ESTABLECIMIENTO DEL CONTEXTO

6.1.1 ACTIVOS DEL SISTEMA DE INFORMACIÓN ACADÉMICA

El sistema de información académica de la Universidad de Pamplona se llama ACADEMUSOFT, aunque también es conocido como el Campus TI. Los procesos que se llevan a cabo a través de él son:

- Consulta de datos personales de estudiantes y docentes (hoja de vida)
- Consulta de información académica (materias, horarios y notas) de los estudiantes
- Registro de notas de los estudiantes por parte de los docentes
- Consulta de información financiera del estudiante (matrícula financiera, deudas)
- Modificación de datos personales por parte de estudiantes y docentes
- Introducción de datos personales de estudiantes y docentes por parte de los administrativos
- Modificación de información académica por parte de los administrativos
- Activación/desactivación de privilegios en la plataforma ACADEMUSOFT por parte del personal del CIADTI (Centro de Investigación Aplicada y Desarrollo en Tecnologías de Información)

Los activos involucrados en estos procesos se pueden clasificar de la siguiente manera:

1. **Activos de Información:**
    - **Hardware:**
        - Servidor de Base de Datos de Información Académica y de Autenticación.
        - Dispositivos utilizados por los usuarios para acceder a ACADEMUSOFT (Teléfonos Móviles , PCs, portátiles, etc.).
        - Dispositivos de almacenamiento de información de los usuarios (USBs, Tablets, Teléfonos Móviles, etc.).

- **Software:**
    - Servicio de Autenticación al campus TI.
    - Base de Datos de Información Académica con su respectiva interfaz gráfica (ACADEMUSOFT).
    - Navegador WEB de los usuarios.
- **Red:**
    - Canal de Comunicación Cliente/Servidor.

2. **Personal:**
    - Estudiantes
    - Docentes
    - Administrativos
    - Personal CIADTI
3. **Sitio:**
    - Centro de datos donde están el servidor de base de datos de información académica y el de autenticación.
    - Lugar desde donde consultan los usuarios ACADEMUSOFT (Café internet, domicilio, universidad).
4. **Organización:**
    - Imagen y Reputación de la Institución.
    - Políticas del Sistema de Información Académica.

6.1.2 FUNCIONES DE LOS ACTIVOS

1. **Activos de Información:**
    - **Hardware:**
        - **Servidor de Base de Datos de Información Académica y de Autenticación:** Su función es albergar la base de datos de información académica y el sistema de autenticación de ACADEMUSOFT, así como permitirle a los usuarios el acceso a estos servicios a través de Internet, para que lleven a cabo los diferentes procesos que permite la plataforma.

- **Dispositivos utilizados por los usuarios para acceder a ACADEMUSOFT (Teléfonos Móviles , PCs, portátiles, etc.):** Su función es permitir el uso del navegador web a los usuarios para acceder a ACADEMUSOFT.
- **Dispositivos de almacenamiento de información de los usuarios (USBs, Tablets, Teléfonos Móviles, etc.):** Su función es permitir a los usuarios almacenar la información que suben y descargan de ACADEMUSOFT.

- **Software:**
  - **Servicio de Autenticación al campus TI:** Su función es verificar si el nombre de usuario y contraseña introducidos son correctos, para permitir o denegar el acceso a los usuarios al sistema de información académica.
  - **Base de Datos de Información Académica con su respectiva interfaz gráfica (ACADEMUSOFT):** Su función es mostrar la información de la base de datos de información académica, y permitir su modificación y descarga.
  - **Navegador WEB de los usuarios**: Su función es posibilitar el acceso vía WEB a ACADEMUSOFT, además de visualizar y modificar la información en él almacenada.

- **Red:**
  - **Canal de Comunicación Cliente/Servidor:** Su función es transportar la información que comparten entre sí los servidores y los usuarios.

2. **Personal:**
   - **Estudiantes:** Su función es consultar y descargar sus notas, horarios, materias y matrícula financiera, así como modificar sus datos personales.
   - **Docentes:** Su función es consultar y descargar las listas de sus estudiantes y las notas de sus cursos, consultar la evaluación docente, ingresar las notas de sus cursos y modificar sus datos personales.
   - **Administrativos:** Su función es introducir ciertos datos personales de los estudiantes y docentes, así como modificar cierta información académica.
   - **Personal CIADTI:** Su función es activar/desactivar los privilegios de los usuarios en la plataforma ACADEMUSOFT y programar el software de la plataforma.
3. **Sitio:**

- **Centro de datos donde están el servidor de base de datos de información académica y el de autenticación**: Su función es albergar y proteger los servidores y dispositivos de red.

- **Lugar desde donde consultan los usuarios ACADEMUSOFT (Café internet, domicilio, universidad):** Su función es albergar los dispositivos que les permiten a los usuarios acceder a ACADEMUSOFT.

4. **Organización:**

- **Imagen y Reputación de la Institución:** Su función es mejorar cada día para que la Universidad de Pamplona pueda vender la plataforma ACADEMUSOFT a otras instituciones educativas.

- **Políticas del Sistema de Información Académica:** Su función es establecer los lineamientos de funcionamiento del sistema de información académica.

6.1.3 RESPONSABLES DE LOS ACTIVOS

1. **Activos de Información:**

- **Hardware:**

  - Servidor de Base de Datos de Información Académica y de Autenticación. **Responsable:** CIADTI

  - Dispositivos utilizados por los usuarios para acceder a ACADEMUSOFT (Teléfonos Móviles , PCs, portátiles, etc.). **Responsable:** Usuario

  - Dispositivos de almacenamiento de información de los usuarios (USBs, Tablets, Teléfonos Móviles, etc.). **Responsable:** Usuario

- **Software:**

  - Servicio de Autenticación al campus TI. **Responsable:** CIADTI

  - Base de Datos de Información Académica con su respectiva interfaz gráfica (ACADEMUSOFT). **Responsable:** CIADTI

  - Navegador WEB de los usuarios. **Responsable:** Usuario

- **Red:**

  - Canal de Comunicación Cliente/Servidor. **Responsable:** CIADTI

2. **Personal:**

- Estudiantes. **Responsable:** Usuario

- Docentes. **Responsable:** Usuario
- Administrativos. **Responsable:** Usuario
- Personal CIADTI. **Responsable:** Usuario

3. **Sitio:**
   - Centro de datos donde están el servidor de base de datos de información académica y el de autenticación. **Responsable:** CIADTI
   - Lugar desde donde consultan los usuarios ACADEMUSOFT (Café internet, domicilio, universidad). **Responsable:** Usuario
4. **Organización:**
   - Imagen y Reputación de la Institución. **Responsable:** Universidad
   - Políticas del Sistema de Información Académica. **Responsable:** CIADTI y Directivas de la Universidad

6.1.4 INFORMACIÓN CONFIDENCIAL Y NIVEL DE PRIVACIDAD

La información confidencial manejada en ACADEMUSOFT es:

- Datos personales y familiares de estudiantes y docentes. **Nivel de privacidad:** Alto
- Información profesional de estudiantes y docentes. **Nivel de privacidad:** Medio
- Información académica del estudiante (notas, materias, horarios). **Nivel de privacidad:** Alto
- Estímulos dados a estudiantes y docentes. **Nivel de privacidad:** Medio
- Información financiera del estudiante. **Nivel de privacidad:** Alto

6.1.5 LEYES DE SEGURIDAD INFORMÁTICAS APLICABLES

La ley a nivel colombiano que aplica directamente al sistema de información académica es la Ley 1581 de 2012 (Protección de Datos Personales), ya que en ella se establecen todos los lineamientos a tener en cuenta para manejar adecuadamente los datos personales de los usuarios.

6.1.6 POLÍTICAS DE SEGURIDAD INSTITUCIONALES APLICABLES

Las políticas de seguridad institucionales apenas se están definiendo, así que todavía no se tiene claro qué tratamiento se debe dar a los activos de la institución

6.1.7 EXPECTATIVAS DE LOS USUARIOS

Aunque no se contó con el tiempo suficiente para realizar encuestas a los diferentes tipos de usuarios para conocer sus expectativas sobre el funcionamiento y seguridad de ACADEMUSOFT, como usuarias que hemos sido del sistema durante varios años, desempeñando los roles de docente y estudiante, podemos decir que, en cuanto a su funcionamiento, esperamos que el sistema esté disponible a cualquier hora, es decir, que no se presenten caídas del servicio, y que permita realizar de manera fácil todas las tareas para las que es utilizado. En cuanto a su seguridad, esperamos que los datos personales y la información académica no sean vistos y ni mucho menos modificados por personas no autorizadas.

El defraudar las expectativas de los usuarios, podría disminuir la confianza de los usuarios en ACADEMUSOFT, ocasionar comentarios negativos con respecto al sistema y hasta demandas contra la institución, lo que afectaría enormemente la imagen y reputación de la institución.

6.1.8 ALCANCE DEL ANÁLISIS DE RIESGOS

En el análisis de riesgos se van a tener en cuenta todos los activos del sistema de información académica indenficados previamente.

6.2 PASO 2: IDENTIFICACIÓN DE RIESGOS

6.2.1 VALORACIÓN DE LOS ACTIVOS

Para valorar los activos, se utilizó la siguiente escala de Likert, que es semi-cuantitativa:

- 1: Muy bajo
- 2: Bajo
- 3: Medio
- 4: Alto
- 5: Muy alto

En la Tabla 29 se determina el impacto que tendría la pérdida de disponibilidad, integridad y confidencialidad de los activos para ACADEMUSOFT y la Universidad de Pamplona.

Tabla 29. Valoración de Activos

ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	TOTAL	ORDEN DE PRIORIDAD
HARDWARE					
Servidor de Base de Datos de Información Académica y de Autenticación	5 (Si este servidor no está disponible se retrasan los procesos académicos)	5 (Una pérdida de integridad en este servidor puede ocasionar pérdida parcial o total de la información almacenada en él)	5 (Ya que interesa la información personal de los usuarios, el que alguien viole la confidencialidad de dicha información pone en riesgo la imagen y reputación de la institución)	5	**2**
Dispositivos Utilizados por los Usuarios para Acceder a ACADEMUSOFT (Teléfonos Móviles, PCs, Portátiles, etc.)	1 (No afecta el desarrollo de los procesos académicos pues existen diferentes alternativas de equipos para acceder)	1 (No tiene ningún efecto en los procesos académicos de la institución)	4 (Un atacante podría obtener las contraseñas de los usuarios si estos utilizan un equipo público, a través de un screenlogger, lo que permitiría un ataque de suplantación de identidad)	2	**14**
Dispositivos de Almacenamiento de Información de los Usuarios (USBs, Tablets, Teléfonos Móviles, etc.)	1 (No afecta debido a que no tiene influencia dentro de los procesos académicos)	1 (Si se daña la información almacenada en estos dispositivos descargada de ACADEMUSOFT, dicha información se puede	5 (Si se guarda en estos dispositivos información personal y confidencial, esto puede acarrear demandas injustas contra la institución por parte de los usuarios por revelación indebida	2.33	**12**

ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	TOTAL	ORDEN DE PRIORIDAD
		recuperar de la base de datos, así que no sería crítica esa pérdida)	de dicha información, o extorsiones por parte de terceros)		
SOFTWARE					
Servicio de Autenticación al Campus TI	4 (Depende del tiempo en que no esté disponible ya que si es por un largo lapso de tiempo entorpece los procesos normales de ingreso, consulta y modificación que tienen los usuarios.)	5 (Una pérdida de integridad de este servicio podría ser el cambio no autorizado de contraseñas, lo que propiciaría ataques de suplantación de identidad)	5 (Si las contraseñas se almacenan en claro dentro del servidor cualquiera que obtenga esta tabla puede acceder al campus y realizar cambios significativos de acuerdo a los privilegios que tenga el usuario.)	4.67	**7**
Base de Datos de Información Académica con su Respectiva Interfaz Gráfica (ACADEMUSOFT)	5 (Si no está disponible entorpece los procesos académicos y administrativos que son utilizados constantemente)	5 (Cuando existen modificaciones irregulares de datos personales y notas se afecta seriamente la imagen de la institución y se pierde la confianza de los usuarios del sistema)	5 (La información académica está catalogada como confidencial y nadie, solo el propietario, puede acceder a ella por lo que una pérdida de confidencialidad de la misma puede traer demandas contra la institución, lo que afecta su imagen ante la sociedad)	5	**1**

ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	TOTAL	ORDEN DE PRIORIDAD
Navegador WEB de los Usuarios	1 (En caso de daño del navegador, el usuario puede descargar gratis de Internet el software y solucionar el problema fácilmente)	3 (Modificar la configuración del navegador puede tener cierto impacto pues los rastros que deja el usuario en el equipo pueden ser utilizados por un atacante para obtener información y realizar luego algún tipo de ataque activo)	1 (Por ser un software de uso libre para los usuarios, no tiene implicaciones de confidencialidad)	1.67	**15**
RED					
Canal de Comunicación Cliente/Servidor	3 (La mayoría de los usuarios no acceden con frecuencia al campus, por lo que no necesitan de un canal de comunicación que esté siempre disponible. Son los administrativos los que requieren una mayor disponibilidad para realizar ciertos procesos	5 (Es de gran impacto ya que la modificación de la información que viaja por este canal, por parte personas no autorizadas, puede ocasionar que los usuarios visualicen información falsa o que las modificaciones que se hagan a la información	5 (Es indispensable que la información personal almacenada en el campus, no pueda ser vista por usuarios no autorizados mientras viaja por la red)	4.33	**8**

ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	TOTAL	ORDEN DE PRIORIDAD
	académicos)	almacenada en el campus no lleguen correctamente al servidor)			
SITIO					
Centro de Datos Donde Están el Servidor de Base de Datos de Información Académica y el de Autenticación	5 (Esté centro debe estar disponible en todo momento pues los servidores deben estar funcionando todo el tiempo)	5 (Este lugar debe permanecer en excelentes condiciones de iluminación, humedad y con aire acondicionado para garantizar el buen funcionamiento de los equipos y así prolongar su vida útil.)	5 (Se debe restringir el acceso a este centro solo a personal autorizado, porque el ingreso de personas no autorizadas puede ocasionar el robo o modificación de información y el daño de los equipos.)	5	**5**
Lugar desde Donde Consultan los Usuarios ACADEMUSOFT (Café Internet, Domicilio, Universidad)	2 (No afecta demasiado, ya que los usuarios cuentan con diferentes alternativas de lugar de acceso)	1 (El que el lugar de acceso esté en malas condiciones no afecta siempre y cuando el dispositivo de acceso funcione)	3 (Los usuarios deben ser precavidos con las personas que los observen cuando ingresan al campus ya que puede verse comprometida su contraseña y su información personal.)	2.33	**13**
ORGANIZACIÓN					
Imagen y	5	5	1	3.67	**9**

ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	TOTAL	ORDEN DE PRIORIDAD
Reputación de la Institución	(El que la institución no disponga de una imagen y reputación a nivel nacional e internacional la perjudica en los campos económico, académico y científico)	(Es de relevancia que la imagen y la reputación sean buenas ante la sociedad en todo momento, el que decaiga la imagen de la institución puede generar la reducción del número de estudiantes en los diferentes programas y por lo tanto pérdidas económicas)	(Por ser una institución de carácter público su imagen y reputación deben ser conocidas a nivel nacional e internacional, por lo que no interesa en este caso la confidencialidad)		
Políticas del Sistema de Información Académica	5 (Si no se cuenta con políticas para el manejo y organización del sistema de información académica, las personas no conocerían sus funciones y responsabilidades y se presentaría un caos en los procesos académicos, que perjudicaría enormemente a	5 (Es de suma importancia que las políticas que rigen el sistema de información académica sean los más estables y claras posibles, pues un cambio frecuente en estas políticas puede ser visto como una falta de seriedad por parte de la	1 (Las políticas del sistema de información académica deben ser públicas y conocidas por todos los usuarios)	3.67	**11**

ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	TOTAL	ORDEN DE PRIORIDAD
	la institución)	institución			

Para la valoración de los activos de personal, se utiliza la misma escala de Likert utilizada para los otros activos, para determinar el impacto que tendría para la Universidad de Pamplona, la falta de conocimientos, aptitudes y actitudes por parte del personal en el manejo del Sistema de Información Académica (ver Tabla 30):

Tabla 30. Valoración de Activos de Personal

ACTIVOS	CONOCIMIENTOS	APTITUDES	ACTITUDES	TOTAL	ORDEN DE PRIORIDAD
Estudiantes	3 (Aunque el estudiante no sepa cómo manejar el sistema, existen documentos de ayuda para el ingreso y manejo de la plataforma lo cual contribuye a que los usuarios no tengan que solicitar ayuda a otras personas, en la mayoría de los casos. Además, los estudiantes solo pueden consultar la información del sistema, no modificarla, por lo que su falta de conocimientos no tiene incidencia en el desarrollo normal de los procesos	4 (La falta de aptitudes en el manejo del sistema contribuye a que tengan que recurrir a ayuda externa por lo que el mismo usuario expone su información personal a terceros.)	4 (El no tomar precauciones en el momento de ingreso al sistema o el permitir que otras personas ingresen en su nombre para buscar algún tipo de información son malas prácticas que hacen que la información personal se vea expuesta)	3.67	**10**

ACTIVOS	CONOCIMIENTOS	APTITUDES	ACTITUDES	TOTAL	ORDEN DE PRIORIDAD
	académicos)				
Docentes	4 (Aunque el docente no sepa cómo manejar el sistema, cuenta con las mismas ayudas de ingreso y manejo del sistema que los estudiantes lo cual facilita su manejo sin conocimientos previos, sin embargo los docentes deben ingresar las notas en unas fechas determinadas y al no realizarlo se retrasan los procesos académicos)	5 (La falta de aptitudes en el manejo del sistema contribuye a que tengan que recurrir a ayuda externa por lo que el mismo usuario expone su contraseña e información personal a terceros)	5 (El no tomar precauciones en el momento de ingreso al sistema o el permitir que otras personas ingresen en su nombre para buscar algún tipo de información son malas prácticas que hacen que la información personal se vea expuesta y aumenta el impacto porque los docentes pueden modificar la información en el sistema)	4.67	**6**
Administrativos	5 (Aunque los administrativos tienen el mismo tipo de ayudas de ingreso y manejo del sistema que los estudiantes y docentes, pueden realizar muchas	5 (Por no existir un plan de selección del personal administrativo basado en el perfil profesional, se contrata mano	5 (La alta rotación del personal en los diferentes periodos académicos da como resultado la poca pertenencia y responsabilidad	5	**4**

ACTIVOS	CONOCIMIENTOS	APTITUDES	ACTITUDES	TOTAL	ORDEN DE PRIORIDAD
	más tareas de modificación de la información, y cuando cuentan con muchos privilegios dichas ayudas se quedan cortas y definitivamente se necesitan tener conocimiento del sistema para no retrasar los procesos académicos))	de obra no calificada, cuyas aptitudes en el manejo de sistemas de información son limitadas lo que acarrea errores, inconsistencias y mal manejo de la información.)	para con los roles designados, lo que hace que no se tenga el cuidado adecuado con la información almacenada en ACADEMUSOFT)		
Personal CIADTI	5 (Ya que este personal es quien programa y configura el sistema, debe tener conocimientos claros y amplios sobre el desarrollo de software seguro, las políticas de seguridad de la institución, y la configuración adecuada de los diferentes privilegios y funciones)	5 (La experiencia es la clave para que un proceso tome la madurez necesaria , el ingreso de personal nuevo, entre ellos pasantes, hace que los procesos iniciados, que implican medidas de seguridad, queden a la deriva)	5 (La rotación de personal hace que el CIADTI sea un trampolín para ingreso de funcionarios a nuevas instituciones. Esta rotación, junto con el tipo de contratación, hace que la actitud del personal no sea la más adecuada en cuanto al manejo y cuidado que la información y el	5	**3**

ACTIVOS	CONOCIMIENTOS	APTITUDES	ACTITUDES	TOTAL	ORDEN DE PRIORIDAD
			sistema requieren)		

Los resultados obtenidos en la Tabla 29 y la Tabla 30 indican que el orden de los activos por grado de importancia para el sistema de información académica ACADEMUSOFT es:

1. Base de Datos de Información Académica con su Respectiva Interfaz Gráfica (ACADEMUSOFT)
2. Servidor de Base de Datos de Información Académica y de Autenticación
3. Personal CIADTI
4. Administrativos
5. Centro de Datos Donde Están el Servidor de Base de Datos de Información Académica y el de Autenticación
6. Docentes
7. Servicio de Autenticación al Campus TI
8. Canal de Comunicación Cliente/Servidor
9. Imagen y Reputación de la Institución
10. Estudiantes
11. Políticas del Sistema de Información Académica
12. Dispositivos de Almacenamiento de Información de los Usuarios
13. Lugar desde donde Consultan los Usuarios ACADEMUSOFT
14. Dispositivos Utilizados por los Usuarios para Acceder a ACADEMUSOFT
15. Navegador WEB de los Usuarios

Este orden ayudará a priorizar los riesgos cuando tengan el mismo valor.

6.2.2 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

A continuación se determinan las diferentes vulnerabilidades y amenazas a las que se ven expuestos los activos identificados anteriormente (ver Tabla 31).

Tabla 31. Amenazas y Vulnerabilidades

ACTIVOS	VULNERABILIDADES	AMENAZAS
HARDWARE		
Servidor de Base de Datos de Información Académica y de Autenticación	Mantenimiento insuficiente	Fallas en el funcionamiento del hardware y software del servidor
	Ausencia de esquemas de reemplazo periódico.	Cumplimiento del tiempo de vida útil del servidor y sus partes
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, humedad.
	Sensibilidad a la radiación electromagnética.	Radiación electromagnética.
	Falta de control de los cambios hechos en la configuración del servidor	Error en el uso y explotación de agujeros de seguridad
	Susceptibilidad a las variaciones de voltaje (falta de regulador y UPS)	Pérdida del suministro de energía y picos de energía.
	Falta de puntos de restauración del sistema	Falla en el sistema operativo
	Falta de realización periódica de copias de respaldo	Fallo del disco duro
	Falta de contraseña robusta de administrador	Ingreso de usuarios no autorizados
	Falta de condiciones de refrigeración adecuadas.	Sobrecalentamiento del procesador y salida de funcionamiento del servidor.
	Ausencia de terminación de sesión cuando se abandona el servidor	Ataque de suplantación de identidad
	Acceso de múltiples personas al servidor	Robo, modificación y borrado de información personal de los usuarios
	Copia no controlada de la información del servidor	Robo de información personal de los usuarios
	Ausencia de revisión periódica de las bitácoras (logs) del servidor y de monitoreo del sistema en busca de	Ataques pasivos y activos al sistema de información académica

ACTIVOS	VULNERABILIDADES	AMENAZAS
	fallas e incidentes de seguridad	
Dispositivos utilizados por los usuarios para acceder a ACADEMUSOFT (Teléfonos Móviles, PCs, portátiles, etc.)	Descarga descontrolada e instalación de software libre	Malware (virus, troyanos, gusanos, etc.)
	Mantenimiento insuficiente.	Fallas en el funcionamiento del dispositivo.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, humedad.
	Sensibilidad a la radiación electromagnética.	Radiación electromagnética.
	Uso compartido del dispositivo	Robo, borrado y modificación de la información.
	Ausencia de terminación de sesión cuando se abandona la estación de trabajo	Suplantación de Identidad
Dispositivos de almacenamiento de información de los usuarios (USB, Tablets, Teléfonos Móviles, etc.)	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, humedad.
	Sensibilidad a la radiación electromagnética.	Radiación electromagnética.
	Ingreso de dispositivos en equipos no protegidos	Malware (virus, troyanos, gusanos, etc.)
	Descuido del lugar donde se dejan los dispositivos	Robo del dispositivo y de la información.
	Ausencia de copias de respaldo	Daño del dispositivo y pérdida de la información
SOFTWARE		
Servicio de Autenticación al campus TI	Falta de mecanismo de autenticación fuerte, falta de complejidad en las contraseñas, y ausencia de límite de intentos de autenticación	Ataques de robo y suplantación de identidad

ACTIVOS	VULNERABILIDADES	AMENAZAS
	Usuario y contraseña viajando en claro por la red	Sniffing
	Almacenamiento en claro de las contraseñas (tablas de contraseñas sin protección)	Obtención de las contraseñas de acceso de los usuarios y falsificación de derechos)
	Fallas en el diseño e implementación del software que crean agujeros de seguridad	Explotación de agujeros de seguridad
	Interfaz de usuario compleja que causa demora en el ingreso al campus y solicitud de ayuda para ingresar	Ataques de Eavesdropping e Ingeniería Social
Base de Datos de Información Académica (ACADEMUSOFT)	Falta de mecanismo de autenticación fuerte	Ataques de robo y suplantación de identidad
	Información viajando en claro por la red.	Sniffing
	Almacenamiento sin la debida protección de la información académica	Robo, borrado, modificación de la información.
	Falta de copias de respaldo.	Pérdida de la Información.
	Defectos en el software e insuficiencia de pruebas del mismo	Explotación de agujeros de seguridad
	Interfaz de usuario compleja	Error en el uso
	Ausencia de control de cambios eficaz, que permite otorgar privilegios de manera indiscriminada a ciertos usuarios y falta de roles definidos para los diferentes tipos de usuarios	Abuso de los privilegios de acceso
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
Navegador WEB de	Falta de configuración del	Ataques de robo de información

ACTIVOS	VULNERABILIDADES	AMENAZAS
los usuarios	navegador en cuanto a: bloqueo de cookies, almacenamiento de contraseñas, nivel de seguridad, almacenamiento de historial, etc.	gracias a rastros de navegación
	Desbordamiento de Buffer	Ataques que causan inestabilidad en el navegador
	Ausencia de terminación de sesión cuando se abandona la estación de trabajo	Ataques de suplantación de identidad
	Instalación y activación indiscriminada de complementos	Control remoto de los recursos de la estación de trabajo
RED		
Canal de Comunicación Cliente/Servidor	Información viajando en claro por el canal.	Sniffing
	Conexiones a red pública sin protección	Sniffing MITM (Man in the Middle) Espionaje remoto
	Gestión inadecuada de la red	Congestión en la red y saturación del sistema de información
SITIO		
Centro de Datos Donde Están el Servidor de Base de Datos de Información Académica y el de Autenticación	Falta de aire acondicionado	Recalentamiento de los equipos
	Presencia de humedad, polvo y suciedad.	Susceptibilidad de los equipos a la humedad, el polvo y la suciedad.
	Falta de control de acceso al centro de datos.	Robo, borrado y modificación de la información. Robo y daño de equipos.
	Red eléctrica inestable	Pérdida del suministro de energía y picos de energía
	Ubicación en un área susceptible a inundación y desastres naturales	Inundación y desastres naturales

ACTIVOS	VULNERABILIDADES	AMENAZAS
	Falta de plan de contingencia	Incidentes o fallas inesperados
Lugar desde donde consultan los usuarios ACADEMUSOFT (Café internet, domicilio, universidad)	Falta de control de acceso y seguridad física en los sitios públicos	Eavesdropping (atacante fisgonea la contraseña y la información del campus) Instalación de herramientas de ataque ocultas por parte de atacantes Robo de dispositivos de almacenamiento
	Red eléctrica inestable	Daño de dispositivos de almacenamiento
ORGANIZACIÓN		
Imagen y Reputación de la Institución	Corrupción	Criminalidad (chantaje, robo, hurto, espionaje)
	Dar percepción errónea de seguridad a los usuarios del campus	Decepción de los usuarios por fallas de seguridad
Políticas del Sistema de Información Académica	Falta de políticas de seguridad del sistema de información académica, donde se especifique claramente cuáles son los activos importantes para la institución, quien está a cargo de cada activo, qué medidas de seguridad se deben implantar en cada uno y qué sanciones se aplicarán en caso de algún incidente	Error en el uso de los activos del sistema de información académica
	Ausencia de auditorías (supervisiones) regulares del sistema de información académica y los empleados	Mal funcionamiento del sistema e incumplimiento de las funciones por parte del personal
	Ausencia de procedimientos de identificación y valoración de riesgos	Uso de medidas de seguridad ineficaces

ACTIVOS	VULNERABILIDADES	AMENAZAS
	Falta de divulgación de las políticas de seguridad del sistema de información académica	Error en el uso de los activos del sistema de información académica
	Ausencia de procedimiento formal para el control de la documentación del SGSI	Inconsistencias en la documentación del SGSI
	Ausencia o insuficiencia en las disposiciones, con respecto a la seguridad de la información, en los contratos con los empleados	Robo, pérdida o modificación de la información y espionaje
	Ausencia de procedimiento formal para el retiro de usuarios del sistema y revisión periódica (supervisión) de los derechos de acceso, así como la asignación de dicha responsabilidad a un cargo específico	Abuso de los privilegios de acceso al sistema de información académica
PERSONAL		
Estudiantes	Falta de confidencialidad y complejidad de la contraseña de acceso al sistema de información académica	Ataques de robo y suplantación de identidad
	Desconocimiento de las políticas de seguridad del sistema de información académica y falta de capacitación y concientización en seguridad	Error en el uso del sistema de información académica y daño o pérdida de la información.
	Ingreso al sistema de información académica desde sitios públicos y falta de precauciones de seguridad al ingresar al campus	Ataques de robo y suplantación de identidad e ingeniería social
	Falta de confidencialidad de la información que descarga del sistema de información académica	Obtención de historial académico por personas no autorizadas

ACTIVOS	VULNERABILIDADES	AMENAZAS
Docentes	Falta de confidencialidad y complejidad de la contraseña de acceso al sistema de información académica	Ataques de robo y suplantación de identidad
	Desconocimiento de las políticas de seguridad del sistema de información académica y falta de capacitación y concientización en seguridad	Error en el uso del sistema de información académica y daño o pérdida de la información.
	Ingreso al sistema de información académica desde sitios públicos y falta de precauciones de seguridad al ingresar al campus	Ataques de robo y suplantación de identidad, e ingeniería social
	Almacenamiento desprotegido de la información que descarga y sube al campus TI	Obtención de notas e historial académico de los estudiantes e información personal por personas no autorizadas
Administrativos	Falta de políticas, capacitación y concientización en cuanto al adecuado uso del sistema y su seguridad	Error en el uso del sistema de información académica y de la información personal almacenada en él
	Falta de personal suficiente y sobrecarga de trabajo del personal existente	Incumplimiento de las funciones o realización de las tareas a medias y atraso de los procesos académicos
	Procedimientos inadecuados de contratación	Mal manejo del sistema de información académica y sus herramientas.
	Ausencia de asignación adecuada de responsabilidades, con respecto a la seguridad de la información, en la descripción de los cargos y en los contratos con los empleados	Robo, pérdida o modificación de la información y espionaje Error en el uso de los activos del sistema de información académica y daño o pérdida de los mismos
	Ausencia de auditorías (supervisiones) regulares de los	Incumplimiento de las funciones por parte del personal y abuso de los

ACTIVOS	VULNERABILIDADES	AMENAZAS
	empleados y su trabajo	privilegios de acceso al sistema de información académica
Personal del CIADTI	Falta de políticas, capacitación y concientización en cuanto al adecuado manejo del sistema y a su seguridad	Error en el uso del sistema de información académica y de la información personal almacenada en él
	Falta de personal suficiente y sobrecarga de trabajo del personal existente	Incumplimiento de las funciones o realización de las tareas a medias y atraso de los procesos académicos
	Procedimientos inadecuados de contratación	Mal manejo del sistema de información académica y sus herramientas.
	Ausencia de asignación adecuada de responsabilidades, con respecto a la seguridad de la información, en la descripción de los cargos y en los contratos con los empleados	Robo, pérdida o modificación de la información y espionaje Error en el uso de los activos del sistema de información académica y daño o pérdida de los mismos, sin que se pueda señalar un responsable de ello.
	Ausencia de auditorías (supervisiones) regulares de los empleados y su trabajo	Incumplimiento de las funciones por parte del personal y abuso de los privilegios de acceso al sistema de información académica

6.3 PASO 3: ANÁLISIS DE RIESGOS

Para determinar la probabilidad de ocurrencia del riesgo se tomaron como base las encuestas aplicadas a docentes y estudiantes (ver Anexo B), la información proporcionada por el personal del CIADTI y los resultados de la VII Encuesta Latinoamericana de Seguridad de la Información (Cano & Saucedo Mesa, 2015) (ver Tabla 32). Además, se utiliza la siguiente escala de Likert:

- **0 – 4.99% :** 1 Muy Bajo.
- **5 – 14.99%:** 2 Bajo.
- **15 – 29.99%:** 3 Medio.

- **30 – 49.99 %:** 4 Alto.
- **50 – 100 %:** 5 Muy Alto.

Para determinar el nivel de riesgos se utiliza la siguiente escala:

- **1 – 4:** **Muy Bajo**
- **5 – 9:** **Bajo**
- **10 – 14:** **Medio**
- **15 – 19:** **Alto**
- **20 – 25:** **Muy Alto**

Tabla 32. Valoración del Riesgo

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
HARDWARE					
Servidor de Base de Datos de Información Académica y de Autenticación	Fallas en el funcionamiento del hardware y el software del servidor	5 (Los daños en el HW y SW debidos al mantenimiento insuficiente tienen un impacto muy alto porque el servidor deja de funcionar durante un lapso de tiempo, ocasionando retrasos en los procesos académicos y algunas veces pérdidas de información. Si no se cuenta con las partes de repuesto o el	3 (Según CIADTI)	**15**	**15**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		software de recuperación adecuados, el tiempo de restablecimiento del servidor será largo, y entre más largo el tiempo más perjudicada se va a ver institución)			
	Cumplimiento del tiempo de vida útil del servidor y sus partes	5 (Los daños en el HW debidos a la ausencia de esquemas de reemplazo periódico tienen un impacto muy alto porque el servidor deja de funcionar durante un lapso de tiempo, ocasionando retrasos en los procesos académicos y algunas veces pérdidas de información.)	2 (Según CIADTI)	**10**	**40**
	Polvo, corrosión, humedad	4 (El polvo no causa mayores daños en los equipos, a	2 (Según CIADTI)	**8**	**53**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		no ser que sea excesivo, pero la humedad y la corrosión, pueden provocar que se dañe el hardware del servidor y lo deje fuera de funcionamiento durante largo tiempo, ocasionando retrasos en los procesos académicos y algunas veces pérdidas de información.)			
	Radiación electromagnética	2 (Se necesitaría una descarga electromagnética muy fuerte para causar pérdida de la información almacenada en el servidor)	1 (Según CIADTI)	**2**	**74**
	Error en el uso y explotación de agujeros de seguridad	5 (Si se configura inadecuadamente el servidor se podrían abrir puertos que aprovechan los	1 (Según CIADTI)	**5**	**59**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		atacantes para hacer diferentes tipos de ataques, lo que podría ocasionar pérdida, robo o modificación de la información. También, los administradores del servidor, al cometer errores en el uso del mismo, pueden borrar accidentalmente información importante)			
	Perdida del suministro de energía y picos de energía	4 (Este tipo de fallos puede sacar de funcionamiento el servidor durante algún tiempo, e incluso dañarlo si el pico de energía es muy alto, lo que ocasionaría retraso en los procesos académicos, y algunas veces pérdida de	4 (Según CIADTI)	**16**	**8**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		información)			
	Falla en el sistema operativo	4 (Al no contar con puntos de restauración recientes, recuperarse de una falla en el sistema operativo podría significar reinstalar el sistema, o volver a configurar las aplicaciones y servicios, por lo que tomaría algún tiempo volver a colocar en funcionamiento el servidor, ocasionando importantes retrasos en los procesos académicos)	2 (Según CIADTI)	**8**	**52**
	Fallo del disco duro	5 (El no tener copia de respaldo de la información académica ocasionaría una gran pérdida de información y para recuperarse	2 (Según CIADTI)	**10**	**39**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		de este incidente se debe invertir mucho tiempo, dinero y esfuerzo, además se podría perder la confianza de los usuarios)			
	Ingreso de usuarios no autorizados	5 (El no contar con una contraseña robusta para ingresar al servidor puede acarrear que usuarios no autorizados ingresen y copien, borren o modifiquen la información académica, lo que puede afectar el buen desarrollo de los procesos académicos, causar inconsistencias y dañar la imagen de la institución)	1 (Según CIADTI)	**5**	**60**
	Sobrecalentamiento del procesador y salida de funcionamiento del servidor.	4 (Si los ventiladores de la CPU no están funcionando	3 (Según CIADTI)	**12**	**27**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		adecuadamente, los técnicos deberán realizarles la limpieza correspondiente o sustituir los ventiladores, lo que tomará algún tiempo para volver a colocar en funcionamiento el servidor. Si el centro de datos no cuenta con aire acondicionado y esa es la causa del sobrecalentamiento, la institución deberá hacer una gran inversión para solucionar el problema)			
	Ataque de suplantación de identidad	5 (El que usuarios no autorizados ingresen al servidor por dejar abierta la sesión del administrador puede ocasionar que copien, borren o	1 (Según CIADTI)	**5**	**61**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		modifiquen la información académica, lo que puede afectar el buen desarrollo de los procesos académicos, causar inconsistencias, dañar la imagen de la institución y demandas de las personas afectadas)			
	Robo, modificación y borrado de información personal de los usuarios	5 (El que muchas personas tengan acceso al servidor con privilegios de administrador puede ocasionar que alguna copie, borre o modifique la información académica, siendo difícil determinar quién lo hizo, lo que puede afectar el buen desarrollo de los procesos académicos, causar inconsistencias y dañar la imagen	1 (Según CIADTI)	**5**	**62**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		de la institución)			
	Robo de información personal de los usuarios	4 (Si cualquier usuario puede hacer copia de la información del servidor o las copias de respaldo del servidor se dejan en un lugar desprotegido, un atacante puede robar la información académica y personal de los usuarios para venderla al mejor postor, lo que puede atentar contra la imagen de la institución)	1 (Según CIADTI)	**4**	**67**
	Ataques pasivos y activos al sistema de información académica	5 (El que los administradores no revisen constantemente los logs del servidor o hagan un monitoreo del sistema en busca de incidentes y fallas, posibilita que los atacantes	2 (Según CIADTI)	**10**	**41**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		tengan el suficiente tiempo para realizar con éxito sus ataques, lo que podría ocasionar copia, borrado o modificación de la información, afectando esto a la imagen de la institución)			
Dispositivos utilizados por los usuarios para acceder a ACADEMUSOFT (Teléfonos Móviles, PCs, portátiles, etc.)	Malware (virus, troyanos, gusanos, etc.)	3 (El software libre puede traer consigo malware que se puede propagar por la red hasta llegar al servidor de ACADEMUSOFT, y si dicho servidor no tiene la suficiente protección podría infectarse y ocasionar pérdidas de información y agujeros de seguridad)	4 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de ocurrencia de los Virus y Caballos de Troya es de 44.6%)	**12**	**33**
	Fallas en el funcionamiento del dispositivo	1 (El que el dispositivo con que cuenta el	3 (Según criterio propio)	**3**	**72**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		usuario falle, puede ocasionarle al usuario pérdida de tiempo, al querer visualizar o modificar información en ACADEMUSOFT, pero no afectará directamente al sistema)			
	Polvo, corrosión, humedad.	1 (El polvo, la corrosión y la humedad van a afectar el correcto funcionamiento del dispositivo del usuario, pero esto no tendrá ninguna influencia sobre el sistema de información académica)	2 (Según criterio propio)	**2**	**78**
	Radiación electromagnética.	1 (Una radiación electromagnética fuerte puede afectar el correcto funcionamiento del dispositivo del	1 (Según criterio propio)	**1**	**80**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		usuario, pero esto no tendrá ninguna influencia sobre el sistema de información académica)			
	Robo, borrado y modificación de la información.	3 (Si el usuario descarga información académica o personal de ACADEMUSOFT y la deja en el dispositivo sin ninguna protección, luego puede acusar injustamente a la institución porque dicha información cayó en manos no deseadas)	3 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de ocurrencia de Pérdida/Fuga de Información Crítica es de 15.5%)	**9**	**50**
	Suplantación de identidad	5 (Si el usuario deja su sesión en ACADEMUSOFT abierta, un atacante puede suplantarlo y aprovechar los privilegios del usuario para	2 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de ocurrencia de la	**10**	**46**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		borrar, copiar o modificar la información, lo cual es bastante grave cuando el usuario es un docente o un administrativo)	Suplantación de Identidad es de 12.7%))		
Dispositivos de almacenamiento de información de los usuarios (USB, Tablets, Teléfonos Móviles, etc.)	Polvo, corrosión, humedad.	1 (El polvo, la corrosión y la humedad van a afectar el correcto funcionamiento del dispositivo de almacenamiento del usuario, pero esto no tendrá ninguna influencia sobre el sistema de información académica)	2 (Según criterio propio)	**2**	**75**
	Radiación electromagnética.	1 (Una radiación electromagnética fuerte puede borrar información del dispositivo del usuario, pero esto no tendrá ninguna influencia sobre	1 (Según criterio propio)	**1**	**79**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		el sistema de información académica)			
	Malware (virus, troyanos, gusanos, etc.)	3 (El malware puede infectar el dispositivo de almacenamiento y con el dispositivo de acceso del usuario y propagarse por la red hasta llegar al servidor de ACADEMUSOFT.]Si dicho servidor no tiene la suficiente protección podría infectarse y ocasionar pérdidas de información y agujeros de seguridad)	4 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de ocurrencia de los Virus y Caballos de Troya es de 44.6%)	**12**	**32**
	Robo del dispositivo y de la información.	3 (Si el usuario descarga información académica o personal de ACADEMUSOFT y la guarda en un dispositivo que	3 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de	**9**	**49**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		luego es robado, más tarde este puede acusar injustamente a la institución porque dicha información cayó en manos no deseadas)	ocurrencia del Robo de Elementos Críticos de Hardware es de 22.5%)		
	Daño del dispositivo y pérdida de la información	1 (El daño en el dispositivo afecta al usuario, pero esto no tendrá ninguna influencia sobre el sistema de información académica)	2 (Según criterio propio)	**2**	**76**
SOFTWARE					
Servicio de Autenticación al campus TI	Ataques de robo y suplantación de identidad	5 (El que esté implementado un método de autenticación débil (usuario/contraseña), no exista un límite de intentos de autenticación y se usen contraseñas débiles, posibilita al atacante	3 (Según el CIADTI)	**15**	**23**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		obtener las credenciales de los diferentes tipos de usuarios y suplantar su identidad, lo que tiene mayor impacto entre más privilegios tenga el usuario. Así, si se trata de un docente, tendrá mayor impacto que si fuera un estudiante, puesto que el docente puede modificar información en el sistema, como las notas, mientras que el estudiante puede sólo visualizarla. Sin embargo, el estudiante tiene acceso a su historial académico y a información personal a través del campus, así que esta información no debería caer en manos de			

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		personas no autorizadas, pues esto podría acarrear demandas contra la institución)			
	Sniffing	4 (El que el usuario y contraseña viajen en claro por la red, le facilitará mucho el trabajo a los atacantes, que pueden luego realizar un ataque de suplantación de identidad y ganar los privilegios del usuario visualizando, modificando o borrando la información almacenada en el sistema de información académica)	1 (Según el CIADTI)	**4**	**69**
	Obtención de las contraseñas de acceso de los usuarios y falsificación de derechos	5 (El que se almacenen en claro las contraseñas en el servidor implicará	1 (Según el CIADTI)	**5**	**64**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		que al tener acceso a dicha tabla se pueda suplantar fácilmente la identidad no sólo de un usuario sino de todos los usuarios que se encuentren en la tabla, por lo que el atacante puede hacer un uso inadecuado de los privilegios de dichos usuarios)			
	Explotación de agujeros de seguridad	5 (Si no se tuvo en cuenta la seguridad al desarrollar el software, este puede tener agujeros que los atacantes usarán como puertas traseras para ingresar al sistema y modificar el SW u obtener las credenciales de los usuarios para perpetrar ataques de suplantación de identidad y	3 (Según el CIADTI)	**15**	**24**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		abusar de sus privilegios)			
	Ataques de Eavesdropping e Ingeniería Social	4 (Cuando la interfaz gráfica es compleja al usuario le tomará más tiempo ingresar al sistema, por lo que un atacante puede husmear la secuencia de caracteres introducidos, e incluso el usuario puede pedir ayuda a un desconocido, que obtendrá su usuario y contraseña y podrá luego suplantar la identidad del mismo)	1 (Según el CIADTI)	**4**	**70**
Base de Datos de Información Académica (ACADEMUSOFT)	Ataques de robo y suplantación de identidad	5 (El no contar con un método de autenticación fuerte, facilita el acceso al sistema por parte de los atacantes, lo que propicia la	2 (Según CIADTI)	**10**	**38**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		suplantación de identidad y el uso de los privilegios de los usuarios para modificar irregularmente las notas e información personal, lo que puede afectar seriamente la imagen de la institución y acarrear demandas contra esta)			
	Sniffing	4 (El que la información viaje en claro por la red, le permitirá a los atacantes obtener el historial académico o los datos personales de los usuarios, sin que sean detectados, información que es privada y que, por tanto, podría acarrear demandas para la institución)	1 (Según el CIADTI)	4	**66**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
	Robo, borrado, modificación de la información.	5 (Si la información en la BBDD de ACADEMUSOFT se almacena en claro y sin ninguna medida para verificar su integridad, cualquiera que obtenga acceso a ella puede robar, borrar o modificar la información, sin ser detectado, lo que puede acarrear inconsistencias, demandas futuras y afectar enormemente la imagen de la institución)	2 (Según CIADTI)	**10**	**35**
	Pérdida de la Información.	5 (El no realizar copias de respaldo periódicas de la información académica, podría ocasionar pérdida de gran cantidad de información,	2 (Según el CIADTI)	**10**	**36**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		información que no siempre se recupera en su totalidad o cuya recuperación toma bastante tiempo, lo que defrauda a los usuarios y afecta grandemente la imagen de la institución)			
	Explotación de agujeros de seguridad	5 (Si no se tuvieron en cuenta las medidas de seguridad al desarrollar el software y no se probó lo suficiente antes de colocarlo en funcionamiento, este puede tener agujeros de seguridad inherentes que los atacantes usarán como puertas traseras para ingresar al sistema y modificar el SW o robar, obtener y modificar la información de	3 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de ocurrencia de los Ataques de Aplicaciones Web es de 16.9%)	**15**	**14**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		los usuarios)			
	Error en el uso	4 (El que ACADEMUSOFT tenga una interfaz compleja hace que el manejo de la plataforma sea complicado sobretodo cuando no se capacita al personal en el uso adecuado de los diferentes privilegios y opciones con que cuentan. Esto causa que los administrativos tengan problemas al subir y consultar información, lo que atrasa los procesos académicos)	2 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de ocurrencia de los Incidentes Relacionados con la Privacidad de los Datos Personales es de 7%)	**8**	**51**
	Abuso de los privilegios de acceso	5 (El otorgar privilegios de manera indiscriminada a los usuarios sin tener un control	1 (Según el CIADTI)	**5**	**58**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		de ello y de cuando se deben revocar dichos privilegios, y la falta de roles definidos para los diferentes tipos de usuarios ha ocasionado que usuarios que ya no hacen parte de la institución modifiquen notas e incluso expidan títulos, lo que desacredita y daña enormemente la imagen de la institución)			
	Mal funcionamiento del software	5 (El que no existan especificaciones completas y claras para los desarrolladores, hace que los nuevos desarrolladores hagan modificaciones sin tener claro el trabajo de los desarrolladores previos y que adicionen nuevos	2 (Según el CIADTI)	**10**	**37**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		agujeros de seguridad al software en lugar de corregir los de las implementaciones anteriores, lo que pueden aprovechar los atacantes para introducirse al sistema y manipularlo.)			
Navegador WEB de los usuarios	Ataques de robo de información gracias a rastros de navegación	2 (Si ACADEMUSOFT utiliza cookies para guardar las preferencias de los usuarios, un atacante puede obtener información personal de los usuarios a través de ellas)	2 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de ocurrencia del Robo de Datos es de 9.9%)	**4**	**71**
	Ataques que causan inestabilidad en el navegador	1 (El desbordamiento de buffer va a ocasionar un mal funcionamiento del navegador, pero no va a afectar al sistema	3 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de	**3**	**73**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		de información académica)	ocurrencia de la Negación de Servicio es de 19.7%)		
	Ataques de suplantación de identidad	4 (Si un usuario no termina su sesión en ACADEMUSOFT antes de dejar el equipo, un atacante puede visualizar, modificar o borrar la información de dicho usuario, y el usuario descuidado puede culpar injustamente de dicho incidente a la institución, lo que afecta la imagen de la misma)	2 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de ocurrencia de la Suplantación de Identidad es de 12.7%)	**8**	**55**
	Control remoto de los recursos de la estación de trabajo	4 (Si el atacante obtiene el control remoto del sistema, puede visualizar todo lo que hace el usuario en el computador,	3 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de	**12**	**34**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		capturar su contraseña y suplantar su identidad, sin que el usuario se percate de ello, ocasionando robo, modificación o borrado de la información)	ocurrencia de la Manipulación de Aplicaciones de Software es de 16.4%)		
RED					
Canal de Comunicación Cliente/Servidor	Sniffing	4 (El que la información viaje en claro por la red, le permitirá a los atacantes obtener la contraseña, el historial académico o los datos personales de los usuarios, sin que sean detectados, información que es privada y cuya obtención y publicación, podría acarrear demandas para la institución, afectando la confianza de los	4 (Según CIADTI)	**16**	**11**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		usuarios y la imagen institucional)			
	Sniffing MITM (Man in the Middle) Espionaje remoto	5 (El hecho que no esté protegido el perímetro de la red de forma adecuada, la hará más vulnerable a ataques externos, que no van a ser detectados oportunamente y que pueden causar robo, borrado o modificación de la información de los usuarios)	1 (Según CIADTI)	**5**	**65**
	Congestión en la red y saturación del sistema de información	4 (El que la topología de la red de la institución no haya sido implementada de manera que evite la congestión y cuellos de botella en determinadas partes de la red, puede ocasionar que los servicios no sean	2 (Según CIADTI)	**8**	**54**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		proporcionados de manera rápida y oportuna, y que incluso la red salga de funcionamiento, lo que retrasará los procesos académicos)			
SITIO					
Centro de Datos Donde Están el Servidor de Base de Datos de Información Académica y el de Autenticación	Recalentamiento de los equipos	4 (El que los equipos se recalienten por falta de aire acondicionado puede causar que los servidores salgan de funcionamiento durante algún tiempo, lo que retrasaría los procesos académicos)	1 (Según CIADTI)	**4**	**68**
	Susceptibilidad de los equipos a la humedad, el polvo y la suciedad.	4 (El polvo no causa mayores daños en los equipos, a no ser que sea excesivo, pero la humedad y la corrosión, pueden provocar	2 (Según CIADTI)	**10**	**43**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		que se dañe el hardware de los servidores y los deje fuera de funcionamiento durante largo tiempo, ocasionando retrasos en los procesos académicos y algunas veces pérdida de información.)			
	Robo, borrado y modificación de la información. Robo y daño de equipos.	5 (Si no se controla el acceso al centro de datos cualquiera que ingrese a él puede tratar de robar, borrar o modificar la información de los servidores, de conectarse a la red para recabar información o de robar o dañar los equipos, lo que acarrearía grandes pérdidas para la institución tanto a nivel económico, como a nivel de su	2 (Según CIADTI)	**10**	**42**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		imagen y se retrasarían los procesos académicos)			
	Pérdida del suministro de energía y picos de energía	4 (Este tipo de fallos puede sacar de funcionamiento los servidores durante algún tiempo, e incluso dañarlos si el pico de energía es muy alto, lo que ocasionaría retraso en los procesos académicos, y algunas veces pérdida de información)	4 (Según CIADTI)	**16**	**10**
	Inundación y desastres naturales	5 (Los desastres naturales pueden destruir completamente el centro de datos y la información, lo que sería una pérdida total de los activos que se encuentran en él)	1 (Según CIADTI)	**5**	**63**
	Incidentes o fallas	5	3	**15**	**20**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
	inesperados	(El no contar con un plan de contingencia donde se indique los pasos a seguir ante los diferentes incidentes y fallas hace que las acciones que se realizan tras ellos sean desordenadas y tome mucho más tiempo la recuperación, lo que retrasaría los procesos académicos)	(Según CIADTI)		
Lugar desde donde consultan los usuarios ACADEMUSOFT (Café internet, domicilio, universidad)	Eavesdropping (atacante fisgonea la contraseña y la información del campus) Instalación de herramientas de ataque ocultas por parte de atacantes Robo de dispositivos de almacenamiento	3 (El que se consulte ACADEMUSOFT desde un sitio público, les brinda a los atacantes un espacio ideal para obtener la información de los usuarios, y los usuarios podrían acusar injustamente a la universidad de	5 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de ocurrencia de las Acciones de Ingeniería Social es de 11.7%, la de la Manipulación de Aplicaciones de Software es	**15**	**26**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		estos incidentes)	de 16.4% y la de el Robo de Elementos Críticos de Hardware es de 22.5%)		
	Daño de dispositivos de almacenamiento	1 (El hecho que se dañen los dispositivos de almacenamiento de los usuarios los puede afectar a ellos pero no afectará al sistema de información académica)	2 (Según criterio propio)	**2**	**77**
ORGANIZACIÓN					
Imagen y Reputación de la Institución	Criminalidad (chantaje, robo, hurto, espionaje)	5 (La corrupción puede afectar grandemente el sistema de información académica, pues los funcionarios se pueden prestar para modificar notas, vender títulos, etc., lo que daña grandemente la imagen de la	2 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de ocurrencia del Fraude Electrónico es de 10.3% y el del Espionaje es 1.4%)	**10**	**44**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		institución)			
	Decepción de los usuarios por fallas de seguridad	4 (El que se dé una percepción errónea de seguridad a los usuarios, por ejemplo, a través del mecanismo de autenticación de ingreso al campus, hace que ellos se defrauden al presentarse incidentes de seguridad, pierdan la confianza en la institución, se reusen a tomar las precauciones adecuadas para cada tipo de activo y hasta demanden a la institución)	3 (Según criterio propio)	**12**	**31**
Políticas del Sistema de Información Académica	Error en el uso de los activos del sistema de información académica	5 (El que no existan políticas de seguridad del sistema de información académica claras, implica que no se	4 (Según el CIADTI: "Aunque no existen políticas formales y lo que existe no se ha socializado	**20**	**7**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		sepa qué activos son importantes para la institución, qué medidas se tienen que tomar para protegerlos y qué sanciones se aplicarían en caso de no cumplir estas políticas, lo que puede causar pérdida y daño de estos activos, retrasos en los procesos académicos y grandes pérdidas para la institución, sin que se pueda señalar un directo responsable)	adecuadamente , el conocimiento que se tiene de los aplicativos por parte del personal disminuye este riesgo.” Además, “no existen procedimientos que explícitamente le den un manejo adecuado” a la información clasificada)		
	Mal funcionamiento del sistema e incumplimiento de las funciones por parte del personal	4 (Si no se hacen auditorías regulares, el sistema funciona mal y los empleados pueden incumplir sus funciones, lo que causa retrasos en los procesos	4 (Según el CIADTI: “La falta de auditorías puede llevar a que la gente caiga reiteradamente en equivocaciones u omisiones, a veces sin	**16**	**13**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		académicos)	saberlo")		
	Uso de medidas de seguridad ineficaces	5 (Si no se identifican y valoran los riesgos, no se implantan medidas de seguridad efectivas que protejan los activos importantes para la institución lo que ocasiona mal funcionamiento del sistema, retraso en los procesos académicos, robo, modificación o pérdida de la información y se defrauda la confianza de los usuarios en el sistema)	2 (Según el CIADTI: "Aunque no existan procedimientos formalizados ante el SIG, si se efectúan acciones formalizadas para controlar ataques y se dispone de herramientas (hardware y software) de aceptable capacidad para la protección")	**10**	**45**
	Error en el uso de los activos del sistema de información académica	5 (El que las políticas de seguridad no sean conocidas por todos los usuarios del sistema,	3 (Según el CIADTI: "Como no existen las políticas no hay un conocimiento	**15**	**25**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		desde el mismo momento en que empiezan a utilizarlo, implica que los usuarios no sepan cuáles son los activos importantes para la institución y las medidas que se deben tener para protegerlos, lo que puede causar pérdida y daño de estos activos, retrasos en los procesos académicos y grandes pérdidas para la institución)	formal. Sin embargo, el conocimiento que se tiene de los aplicativos por parte del personal disminuye este riesgo")		
	Inconsistencias en la documentación del SGSI	3 (El hecho que no exista un sistema de gestión de seguridad de la información bien estructurado y documentado implica que las acciones que se tomen en cuanto a seguridad se van a tomar de manera desordenada y	2 (Según el CIADTI: "Existe documentación en la gran mayoría de procesos del CIADTI, aunque existe cierta debilidad en algunos de los que conciernen al tema de seguridad")	**6**	**57**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		pueden incluso algunas veces ser contradictorias, pues cada dependencia podría implementar sus propias medidas de seguridad, que pueden ser desconocidas para las demás e incompatibles entre sí, lo que causaría confusiones a los usuarios)			
	Robo, pérdida o modificación de la información y espionaje	5 (El hecho que los empleados que están a cargo de la información confidencial de la institución no firmen un acuerdo de confidencialidad al tomar su cargo, implica que ellos pueden hacer mal uso de esa información y que no se puedan tomar acciones legales contra ellos, lo que	4 (Según el CIADTI: "Existen cláusulas en los contratos pero no se han definido mecanismos de seguimiento para controlar este riesgo")	**20**	**6**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		acarrearía grandes pérdidas para la institución)			
	Abuso de los privilegios de acceso al sistema de información académica	5 (El hecho que no se retiren los privilegios a los usuarios una vez cambie la especificación de su cargo o se retiren de la institución, ni se revisen periódicamente los privilegios de los usuarios implica que estos pueden abusar de esos privilegios haciendo, por ejemplo, modificación irregular de notas, lo que implica daños en la imagen de la institución y demandas)	4 (Según el CIADTI: "Aunque existen procedimientos para la administración de los usuarios y se notifican normalmente los eventos de retiro o cambio de funciones de un trabajador, no se aplica (aunque exista) un protocolo formal para retirar los privilegios de un usuario cuando la persona se retira de la Universidad o cambia de asignación. Tampoco existe seguimiento a las acciones realizadas sobre estos eventos")	**20**	**5**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
PERSONAL					
Estudiantes	Ataques de robo y suplantación de identidad	4 (El que la contraseña de ingreso al sistema de información académica no tenga la complejidad y longitud adecuadas y sea conocida por terceros, además que el sistema no tenga configurado un límite de intentos de autenticación, implica que un atacante podría obtener fácilmente la contraseña del estudiante y consultar su historial académico y datos personales, así como descargarlos. Si el atacante hace mal uso de esta información, el estudiante podría acusar injustamente a la	4 (Según la Encuesta realizada a los Estudiantes, el promedio de las preguntas que fueron respondidas erróneamente, que implican la falta de confidencialidad y complejidad de la contraseña (preguntas 1, 2, 3, 6 y 7) es de 37,61%)	**16**	**12**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		institución de publicar su información confidencial, lo que implicaría un daño en la imagen institucional e invertir recursos para probar que el estudiante se equivoca)			
	Error en el uso del sistema de información académica y daño o pérdida de la información.	4 (Si los estudiantes no conocen las políticas de seguridad i del sistema de información académica y no saben nada sobre seguridad informática, van a desconocer qué información del campus es confidencial y qué cuidados deben tener con ella, por lo que podrían culpar a la institución de algún daño en dicha información, sin ser conscientes	5 (Según la Encuesta realizada a los Estudiantes, los resultados de la pregunta 4 indican un desconocimiento de las políticas de seguridad del sistema de información académica de 92.7%)	**20**	**4**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		de su responsabilidad)			
	Ataques de robo y suplantación de identidad e ingeniería social	3 (Al acceder al campus desde sitios públicos y no tomar las precauciones necesarias, algún atacante puede obtener la contraseña del usuario husmeando o engañándolo y suplantar su identidad, para obtener la información del estudiante y realizar algún soborno o publicarla, lo que podría llevar a demandas injustas contra la institución)	3 (Según la Encuesta realizada a los Estudiantes, el promedio de las preguntas que fueron respondidas erróneamente, que implican el ingreso al sistema desde sitios públicos y falta de precauciones de seguridad (preguntas 5 y 8) es de 29,12%)	**9**	**48**
	Obtención de historial académico por personas no autorizadas	3 (El que el estudiante descargue su información del campus TI y no la almacene en un lugar seguro	2 (Según la Encuesta realizada a los Estudiantes, los resultados de la pregunta 10 indican que más	**6**	**56**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		implica que un atacante podría obtener el historial académico del estudiante, que es información confidencial, y publicarlo o sobornar a su propietario, lo que podría acarrear demandas injustas contra la institución)	de una persona tiene acceso a la información descargada del campus en un porcentaje de 14.33%)		
Docentes	Ataques de robo y suplantación de identidad	5 (Ya que el sistema no cuenta con un límite de intentos de autenticación, al no elegir una contraseña larga y compleja, o al dar a conocer su contraseña a terceros, los docentes facilitan la labor de los atacantes, ya que estos podrían obtener esta contraseña y realizar modificación irregular de notas	4 (Según la Encuesta realizada a los Profesores, el promedio de las preguntas que fueron respondidas erróneamente, que implican la falta de confidencialidad y complejidad de la contraseña (preguntas 1, 2,3, 6 y 7) es de 39,86%)	**20**	**3**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		o robar información confidencial del docente y de los estudiantes, lo que afecta enormemente la imagen de la institución y la confianza de los usuarios en el sistema)			
	Error en el uso del sistema de información académica y daño o pérdida de la información.	5 (El que los docentes desconozcan las políticas de seguridad del sistema de información académica y no reciban información y concientización sobre las medidas de seguridad que deben tener con la información confidencial del sistema de información académica, implica que no la usen adecuadamente y que pueda ser	5 (Según la Encuesta realizada a los Profesores, los resultados de la pregunta 4 indican un desconocimiento de las políticas de seguridad del sistema de información académica de 74.47%)	**25**	**1**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		obtenida o modificada por los atacantes, ocasionando demandas contra la institución y mala imagen)			
	Ataques de robo y suplantación de identidad, e ingeniería social	5 (Al acceder al campus desde sitios públicos y no tomar las precauciones necesarias, algún atacante puede obtener la contraseña del usuario husmeando o engañándolo y suplantar su identidad, para modificar notas de manera irregular , robar o borrar información académica de los estudiantes y docentes, lo que podría acarrear demandas contra la institución y mala imagen)	3 (Según la Encuesta realizada a los Profesores, el promedio de las preguntas que fueron respondidas erróneamente, que implican el ingreso al sistema desde sitios públicos y falta de precauciones de seguridad (preguntas 5 y 8) es de 25,31%)	**15**	**22**
	Obtención de notas	5	4	**15**	**21**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
	e historial académico de los estudiantes e información personal por personas no autorizadas	(Si el docente no guarda la información que se descarga o sube al campus en un lugar seguro, que le permita preservar la confidencialidad de la información, esta información puede caer en manos de personas no autorizadas que pueden hacer mal uso de ella, lo que acarrearía demandas contra la institución, pérdida de confianza por parte de los estudiantes en el sistema y mala imagen para la institución)	(Según la Encuesta realizada a los Profesores, el promedio de las preguntas que fueron respondidas erróneamente, que implican el almacenamiento desprotegido de la información que descargan y suben al campus TI (preguntas 10, 11 y 12) es de 32,18%)		
Administrativos	Error en el uso del sistema de información académica y de la información personal almacenada en él.	5 (El que no existan políticas y los administrativos no sean capacitados ni concientizados en cuanto al	3 (Según criterio propio)	**15**	**19**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		adecuado uso del sistema de información académica y las medidas de seguridad que se deben tener con la información almacenada en él, implica que puedan hacer mal uso de ella, abusando de sus privilegios o la pueden dejar expuesta a atacantes que podrían modificarla, borrarla o robarla, lo que puede implicar mala imagen y demandas para la institución, así como pérdida de confianza de los usuarios en el sistema y la institución)			
	Incumplimiento de las funciones o realización de las tareas a medias y atraso de los procesos	3 (El que no haya personal suficiente para realizar las funciones del	3 (Según criterio propio)	**9**	**47**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
	académicos	sistema de información académica hace que se retrasen los procesos académicos)			
	Mal manejo del sistema de información académica y sus herramientas.	4 (Si no se contrata personal con habilidades en el manejo de TIC, estas personas podrían hacer mal uso del sistema y su información, ocasionando pérdida de información, falta de confidencialidad de la misma y retrasos en los procesos académicos)	3 (Según criterio propio)	**12**	**29**
	Robo, pérdida o modificación de la información y espionaje Error en el uso de los activos del sistema de información académica y daño o pérdida de los	5 (Si los contratos no cuentan con una cláusula de confidencialidad y en la definición de los cargos no se especifican cuáles son los activos que son responsabilidad	3 (Según la VII Encuesta Latinoamericana de Seguridad de la Información (2015) el porcentaje de ocurrencia de Pérdida/Fuga de	**15**	**18**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
	mismos	del empleado, este puede hacer mal uso de sus privilegios en el sistema de información académica y legalmente la universidad no podría acusarlo)	Información Crítica es de 15.5%, la del Espionaje es de 1.4% y la de los Incidentes Relacionados con la Privacidad de los Datos Personales es de 7%)		
	Incumplimiento de las funciones por parte del personal y abuso de los privilegios de acceso al sistema de información académica	4 (El que no se realicen auditorías de manera periódica implica que no se puede determinar tempranamente si los empleados están cumpliendo a cabalidad con sus funciones o si están haciendo uso indebido de sus privilegios para aplicar los respectivos correctivos. Esto puede implicar desconfianza de los usuarios, mala imagen y demandas para la	3 (Según criterio propio)	**12**	**30**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		institución)			
Personal CIADTI	Error en el uso del sistema de información académica y de la información personal almacenada en él	5 (El que no existan políticas y el personal del CIADTI no reciba la capacitación y concientización suficiente en cuanto al adecuado manejo del sistema de información académica y su seguridad puede implicar que hagan mal uso del sistema y de la información almacenada en él, sin percatarse de los daños causados, lo que acarrearía demandas por revelación de información confidencial, pérdida de información de los procesos académicos y retraso en los mismos, afectando la imagen de la	4 (Según el CIADTI: "La falta de sensibilización del personal en la cultura de seguridad genera un alto riesgo de manipulación de datos en el sistema de información"	**20**	**2**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		institución)			
	Incumplimiento de las funciones o realización de las tareas a medias y atraso de los procesos académicos	4 (El que no exista personal suficiente para realizar todas las funciones que tienen que ver con el sistema de información académica implica retraso en los procesos académicos, errores en la configuración por no contar con tiempo suficiente, inconformidad del personal, falta de motivación y hasta corrupción)	4 (Según el CIADTI: "Se evidencia sobrecarga en muchas áreas, lo que lleva a realizar las tareas contra el tiempo, conduciendo a un alto riesgo de fallas y omisiones"	**16**	**9**
	Mal manejo del sistema de información académica y sus herramientas.	5 (Es muy importante que se realice un adecuado proceso de selección del personal del CIADTI puesto que deben ser personas honestas y muy confiables, ya que	3 (Según el CIADTI: "Las fallas en los procesos de contratación podrían llevar a vincular personal no idóneo para el desarrollo de las tareas")	**15**	**17**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
		de lo contrario podrían abusar de sus privilegios en el campus y realizar acciones ilegales)			
	Robo, pérdida o modificación de la información y espionaje Error en el uso de los activos del sistema de información académica y daño o pérdida de los mismos, sin que se pueda señalar un responsable de ello.	5 (Es muy importante que el personal del CIADTI firme una cláusula de confidencialidad tan pronto ingrese a trabajar y que sepa qué activos están a cargo suyo, para poder tomar acciones legales contra ellos en caso que revelen información confidencial o hagan mal manejo de ella y de los activos a su cargo)	3 (Según el CIADTI: "En las cláusulas contractuales existen disposiciones al respecto y se asignan con claridad las responsabilidades, pero no hay formalización completa en los procedimientos y en acciones de seguimiento y control")	**15**	**16**
	Incumplimiento de las funciones por parte del personal y abuso de los privilegios de acceso al sistema de información	4 (El que no se realicen auditorías de manera periódica implica que no se puede determinar	3 (Según el CIADTI: "Se realiza supervisión al trabajo pero no hay	**12**	**28**

ACTIVO	AMENAZA	IMPACTO DE AMENAZA	PROBABILIDAD DE OCURRENCIA	MEDICION DEL RIESGO	PRIORIZACIÓN
	académica	tempranamente si los empleados están cumpliendo a cabalidad con sus funciones o si están haciendo uso indebido de sus privilegios para aplicar los respectivos correctivos. Esto puede implicar desconfianza de los usuarios, mala imagen y demandas para la institución)	formalización en acciones de seguimiento y control")		

6.4 PASO 4: PREVENCIÓN DE RIESGOS

El nivel de riesgo y la priorización calculados en el paso anterior, ayudan a identificar qué vulnerabilidades deben ser atendidas con mayor urgencia y cuales pueden esperar. En la Tabla 33, se especifican qué controles pueden aplicarse para prevenir o mitigar cada vulnerabilidad, según lo especifica el paso 4 de la metodología. Se recurrió a la Tabla 31 para determinar qué vulnerabilidad corresponde a cada amenaza.

Tabla 33. Controles a Implementar

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Docentes	**1**	Desconocimiento de las políticas de seguridad del sistema de información académica y falta de capacitación y concientización en seguridad	**A CORTO PLAZO:** *Para el desconocimiento de las políticas:* • Asignar la responsabilidad de la creación e implementación de las estrategias de difusión a un cargo o área específica. • Establecer qué políticas de

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			seguridad aplican a los **docentes**. • Definir la estrategia de difusión de las políticas de seguridad a los **docentes**. • Obtener la aprobación y financiamiento de las estrategias de difusión por parte de las directivas de la institución • Elaborar el material que se utilizará para difundir las políticas *Para la falta de capacitación y concientización:* • Identificar los errores comunes que cometen los **docentes** al manejar el sistema de información académica, y que colocan en riesgo la información almacenada en él. • Definir los objetivos del programa de concientización • Establecer la estructura del programa de concientización, definiendo las diferentes fases que lo conformarán. Se debe tener en cuenta que dicha concientización debe realizarse desde el momento en que el **docente** entra a hacer parte de la institución y luego realizar periódicamente actividades que refuercen y actualicen lo aprendido. • Obtener la aprobación y financiamiento del programa por parte de las directivas de la institución • Seleccionar los temas que se van a abordar durante la concientización. Entre los temas a tener en cuenta están: leyes de delitos informáticos y de protección de datos personales,

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			importancia del rol de los **docentes** en la cadena de seguridad, precauciones que se deben tener antes de acceder al sistema de información acádemica, medidas de seguridad que se deben tener en cuenta mientras se esté consultando el sistema, medidas de seguridad que se deben tener con la información que se descarga o sube al sistema, características mínimas que debe tener la contraseña de acceso al sistema de información académica para que sea segura. • Definir las estrategias y actividades a llevar a cabo para desarrollar los diferentes temas del programa • Elaborar el material que se utilizará en las actividades de concientización • Entrenar al personal que se encargará de realizar la concientización **A LARGO PLAZO** *Para el desconocimiento de las políticas:* • Dar a conocer las políticas de seguridad a los **docentes** • Monitorear las estrategias de difusión • Documentar y evaluar los resultados de las estrategias de difusión • Realizar los cambios que se crean pertinentes en las estrategias de difusión *Para la falta de capacitación y concientización:* • Realizar las actividades de

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			concientización planteadas • Entregar el material elaborado para las diferentes actividades (posters, boletines, etc.) • Monitorear el programa de concientización • Documentar y evaluar los resultados del programa de concientización • Realizar los cambios que se crean pertinentes al programa de concientización
Personal del CIADTI	**2**	Falta de políticas, capacitación y concientización en cuanto al adecuado manejo del sistema y a su seguridad	**A CORTO PLAZO:** *Para la falta de políticas:* • Especificar los activos importantes para el sistema de información académica. • Asignar responsabilidades sobre cada activo a los diferentes cargos y usuarios. • Definir el nivel de seguridad que debe tener cada activo del sistema de información académica. • Clasificar la información manejada dentro del sistema de información académica (nivel de confidencialidad). • Especificar el manejo que se debe dar a cada activo del sistema de información académica según su nivel de seguridad • Especificar las sanciones a aplicar cada vez que se presente un incidente de seguridad determinado. • Determinar si las políticas de seguridad establecidas van en concordancia con las leyes de protección de datos personales y de seguridad informática vigentes a nivel nacional. Si no es así, realizar los ajustes necesarios. • Determinar si las políticas de

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			seguridad establecidas van en concordancia con las políticas de seguridad institucionales. Si no es así, realizar los ajustes necesarios. • Obtener la aprobación de las políticas del sistema de información académica por parte de las directivas de la institución *Para la falta de capacitación y concientización:* • Identificar los errores comunes que comete el **personal del CIADTI** al manejar el sistema de información académica, y que colocan en riesgo la información almacenada en él. • Definir los objetivos del programa de concientización • Establecer la estructura del programa de concientización, definiendo las diferentes fases que lo conformarán. Se debe tener en cuenta que dicha concientización debe realizarse desde el momento en que la persona entra a hacer parte de la institución y luego realizar periódicamente actividades que refuercen y actualicen lo aprendido. • Obtener la aprobación y financiamiento del programa por parte de las directivas de la institución • Seleccionar los temas que se van a abordar durante la concientización. Entre los temas a tener en cuenta están: leyes de delitos informáticos y de protección de datos personales, importancia del rol del **personal del CIADTI** en la cadena de seguridad, precauciones que se deben tener antes de acceder al

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			sistema de información acádemica, medidas de seguridad que se deben tener en cuenta mientras se esté consultando el sistema, medidas de seguridad que se deben tener con la información que se descarga o sube al sistema, características mínimas que debe tener la contraseña de acceso al sistema de información académica para que sea segura. • Definir las estrategias y actividades a llevar a cabo para desarrollar los diferentes temas del programa • Elaborar el material que se utilizará en las actividades de concientización • Entrenar al personal que se encargará de realizar la concientización **A LARGO PLAZO** *Para la falta de políticas:* • Realizar revisiones periódicas de las políticas de seguridad del sistema de información académica, de manera que sean adecuadas para el contexto interno como externo de la institución *Para la falta de capacitación y concientización:* • Realizar las actividades de concientización planteadas • Entregar el material elaborado para las diferentes actividades (posters, boletines, etc.) • Monitorear el programa de concientización • Documentar y evaluar los resultados del programa de

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			concientización • Realizar los cambios que se crean pertinentes al programa de concientización
Docentes	**3**	Falta de confidencialidad y complejidad de la contraseña de acceso al sistema de información académica	**A CORTO PLAZO:** *Para la falta de complejidad:* • Habilitar las directivas de las contraseñas para que se emplee un conjunto amplio de caracteres (mayúsculas, minúsculas, números, símbolos), que la contraseña tenga un número mínimo de caracteres, que haya un historial de contraseñas, que se deba cambiar la contraseña después de un número determinado de días y que se bloqueen las cuentas después de un número determinado de intentos fallidos. *Para la falta de confidencialidad:* • Realizar jornadas de concientización y capacitación a los docentes sobre el uso adecuado del sistema de información académica (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad). **A LARGO PLAZO:** *Para la falta de complejidad:* • Implementar un mecanismo de autenticación fuerte para ingresar al sistema de información académica, que involucre al menos dos factores (algo que se conoce, algo que se posee, algo que se es). • Monitorear el mecanismo de autenticación • Analizar los datos arrojados por el

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			monitoreo del mecanismo de autenticación, a fin de determinar su efectividad
Estudiantes	**4**	Desconocimiento de las políticas de seguridad del sistema de información académica y falta de capacitación y concientización en seguridad	**A CORTO PLAZO:** *Para el desconocimiento de las políticas:* • Asignar la responsabilidad de la creación e implementación de las estrategias de difusión a un cargo o área específica. • Establecer qué políticas de seguridad aplican a los **estudiantes**. • Definir la estrategia de difusión de las políticas de seguridad a los **estudiantes**. • Obtener la aprobación y financiamiento de las estrategias de difusión por parte de las directivas de la institución • Elaborar el material que se utilizará para difundir las políticas *Para la falta de capacitación y concientización:* • Identificar los errores comunes que cometen los **estudiantes** al manejar el sistema de información académica, y que colocan en riesgo la información almacenada en él. • Definir los objetivos del programa de concientización • Establecer la estructura del programa de concientización, definiendo las diferentes fases que lo conformarán. Se debe tener en cuenta que dicha concientización debe realizarse desde el momento en que el **estudiante** entra a hacer parte de la institución y luego realizar

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			periódicamente actividades que refuercen y actualicen lo aprendido. • Obtener la aprobación y financiamiento del programa por parte de las directivas de la institución • Seleccionar los temas que se van a abordar durante la concientización. Entre los temas a tener en cuenta están: leyes de delitos informáticos y de protección de datos personales, importancia del rol de los **estudiantes** en la cadena de seguridad, precauciones que se deben tener antes de acceder al sistema de información acádemica, medidas de seguridad que se deben tener en cuenta mientras se esté consultando el sistema, medidas de seguridad que se deben tener con la información que se descarga o sube al sistema, características mínimas que debe tener la contraseña de acceso al sistema de información académica para que sea segura. • Definir las estrategias y actividades a llevar a cabo para desarrollar los diferentes temas del programa • Elaborar el material que se utilizará en las actividades de concientización • Entrenar al personal que se encargará de realizar la concientización **A LARGO PLAZO** *Para el desconocimiento de las políticas:* • Dar a conocer las políticas de

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			seguridad a los **estudiantes** • Monitorear las estrategias de difusión • Documentar y evaluar los resultados de las estrategias de difusión • Realizar los cambios que se crean pertinentes en las estrategias de difusión *Para la falta de capacitación y concientización:* • Realizar las actividades de concientización planteadas • Entregar el material elaborado para las diferentes actividades (posters, boletines, etc.) • Monitorear el programa de concientización • Documentar y evaluar los resultados del programa de concientización • Realizar los cambios que se crean pertinentes al programa de concientización
Políticas del Sistema de Información Académica	**5**	Ausencia de procedimiento formal para el retiro de usuarios del sistema y revisión periódica (supervisión) de los derechos de acceso, así como la asignación de dicha responsabilidad a un cargo específico	**A CORTO PLAZO:** • Establecer los procedimientos de asignación y retiro de privilegios de acceso al sistema de información académica, de los diferentes tipos de usuarios. • Definir procedimientos formales para la revisión periódica (supervisión) de los derechos de acceso al sistema de información académica de cada usuario **A LARGO PLAZO:** • Revisar periódicamente los derechos de acceso al sistema de información académica de cada usuario.
Políticas del Sistema de	**6**	Ausencia o insuficiencia en las disposiciones, con	**A CORTO PLAZO:** • Establecer los términos y

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Información Académica		respecto a la seguridad de la información, en los contratos con los empleados	condiciones legales de contratación relacionados con la confidencialidad y seguridad de la información gestionada en cada cargo.
Políticas del Sistema de Información Académica	**7**	Falta de políticas de seguridad del sistema de información académica donde se especifique claramente cuáles son los activos importantes para la institución, quien está a cargo de cada activo, qué medidas de seguridad se deben implantar en cada uno y qué sanciones se aplicarán en caso de algún incidente	**A CORTO PLAZO:** • Especificar los activos del sistema de información académica importantes para la institución. • Asignar responsabilidades sobre cada activo a los diferentes cargos y usuarios • Definir el nivel de seguridad que debe tener cada activo del sistema de información académica. • Clasificar la información manejada dentro del sistema de información académica (nivel de confidencialidad). • Especificar el manejo que se debe dar a cada activo del sistema según su nivel de seguridad • Especificar las sanciones a aplicar cada vez que se presente un incidente de seguridad determinado. • Determinar si las políticas de seguridad establecidas van en concordancia con las leyes de protección de datos personales y de seguridad informática vigentes a nivel nacional. Si no es así, realizar los ajustes necesarios. • Determinar si las políticas de seguridad establecidas van en concordancia con las políticas de seguridad institucionales. Si no es así, realizar los ajustes necesarios. • Obtener la aprobación de las políticas por parte de las directivas de la institución **A LARGO PLAZO:** • Realizar revisiones periódicas de

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			las políticas de seguridad del sistema de información académica, de manera que sean adecuadas para el contexto interno como externo de la institución.
Servidor de Base de Datos de Información Académica y de Autenticación	**8**	Susceptibilidad a las variaciones de voltaje (falta de regulador y UPS)	**A CORTO PLAZO:** • Conectar el **servidor** a la red eléctrica a través de un regulador **A LARGO PLAZO:** • Colocar UPS para que el **servidor** no salga de funcionamiento cuando se vaya la energía
Personal del CIADTI	**9**	Falta de personal suficiente y sobrecarga de trabajo del personal existente	**A CORTO PLAZO:** • Definir correctamente los perfiles de las personas a contratar, en cuanto a conocimientos y cualidades humanas que deben tener. • Realizar la selección, contratación y capacitación de personal en las áreas con sobrecarga de trabajo **A LARGO PLAZO:** • Revisar las funciones de cada cargo y determinar si estas funciones deben ser redistribuidas de manera más equitativa para evitar sobrecargas • Realizar los cambios pertinentes en la definición de funciones de los cargos
Centro de Datos Donde Están el Servidor de Datos de Información Académica y el de Autenticación	**10**	Red eléctrica inestable	**A CORTO PLAZO:** • Verificar que la instalación eléctrica del **centro de datos** cuenta con la suficiente potencia y está en óptimas condiciones para soportar todos los equipos • Conectar los equipos del **centro de datos** a través de un regulador a la red eléctrica • Adquirir UPSs para los servidores y dispositivos de red del **centro de datos**, a fin que no salgan de

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			funcionamiento cuando hayan cortes de energía **A LARGO PLAZO:** • Realizar mantenimiento periódico a la instalación eléctrica del **centro de datos**
Canal de Comunicación Cliente/Servidor	**11**	Información viajando en claro por el canal.	**A CORTO PLAZO:** • Cifrar la información mientras viaja por la red, a través de algún protocolo seguro, como SSL/TLS.
Estudiantes	**12**	Falta de confidencialidad y complejidad de la contraseña de acceso al sistema de información académica	**A CORTO PLAZO:** *Para la falta de complejidad:* • Habilitar las directivas de las contraseñas para que se emplee un conjunto amplio de caracteres (mayúsculas, minúsculas, números, símbolos), que la contraseña tenga un número mínimo de caracteres, que haya un historial de contraseñas, que se deba cambiar la contraseña después de un número determinado de días y que se bloqueen las cuentas después de un número determinado de intentos fallidos. *Para la falta de confidencialidad:* • Realizar jornadas de concientización y capacitación a los **estudiantes** sobre el uso adecuado del sistema de información académica (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad). **A LARGO PLAZO:** *Para la falta de complejidad:* • Implementar un mecanismo de autenticación fuerte para ingresar

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			al sistema de información académica, que involucre al menos dos factores (algo que se conoce, algo que se posee, algo que se es). • Monitorear el mecanismo de autenticación • Analizar los datos arrojados por el monitoreo del mecanismo de autenticación, a fin de determinar su efectividad
Políticas del Sistema de Información Académica	**13**	Ausencia de auditorías (supervisiones) regulares del sistema de información académica y los empleados	**A CORTO PLAZO:** • Establecer los objetivos, alcance, criterios y frecuencia de las auditorías que se deben realizar a los activos del sistema de información académica y al personal a cargo de los mismos **A LARGO PLAZO:** • Realizar auditorías periódicas del sistema de información académica como de los empleados y su trabajo
Base de Datos de Información Académica (ACADEMUSOFT)	**14**	Defectos en el software e insuficiencia de pruebas del mismo	**A LARGO PLAZO**: • Realizar pruebas al software, tras hacer modificaciones, antes de colocarlo a disposición de los usuarios
Servidor de Base de Datos de Información Académica y de Autenticación	**15**	Mantenimiento insuficiente	**A CORTO PLAZO:** • Realizar jornadas de concientización y capacitación al **Personal del CIADTI** sobre las medidas de seguridad a tener en cuenta en el **servidor** (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad). **A LARGO PLAZO:** • Realizar periódicamente mantenimiento de software y hardware al **servidor**

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Personal del CIADTI	**16**	Ausencia de asignación adecuada de responsabilidades, con respecto a la seguridad de la información, en la descripción de los cargos y en los contratos con los empleados	**A CORTO PLAZO:** *Para los contratos:* • Establecer los términos y condiciones legales de contratación relacionados con la confidencialidad y seguridad de la información gestionada en cada cargo. *Para los cargos:* • Definir dentro de las funciones de los cargos del personal del CIADTI, quién se encargará de la seguridad de cada uno de los activos del sistema de información académica y las responsabilidades que tiene con dicho activo, como las sanciones en que incurriría si no lo trata adecuadamente. • Verificar que estas responsabilidades se especifiquen claramente en su contrato.
Personal del CIADTI	**17**	Procedimientos inadecuados de contratación	**A CORTO PLAZO:** • Redefinir los pasos que se deben llevar a cabo para la contratación del **personal del CIADTI** • Definir correctamente los perfiles de las personas a contratar, en cuanto a conocimientos y cualidades humanas que deben tener. **A LARGO PLAZO:** • Realizar las entrevistas y las pruebas necesarias para verificar que los candidatos cumplen con los perfiles establecidos • Capacitar adecuadamente al nuevo personal antes de que empiece a desempeñar su cargo

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Administrativos	**18**	Ausencia de asignación adecuada de responsabilidades, con respecto a la seguridad de la información, en la descripción de los cargos y en los contratos con los empleados	**A CORTO PLAZO:** *Para los contratos:* • Establecer los términos y condiciones legales de contratación relacionados con la confidencialidad y seguridad de la información gestionada en cada cargo. *Para los cargos:* • Definir dentro de las funciones de los cargos del personal del CIADTI, quién se encargará de la seguridad de cada uno de los activos del sistema de información académica y las responsabilidades que tiene con dicho activo, como las sanciones en que incurriría si no lo trata adecuadamente. • Verificar que estas responsabilidades se especifiquen claramente en su contrato.
Administrativos	**19**	Falta de políticas, capacitación y concientización en cuanto al adecuado uso del sistema y su seguridad	**A CORTO PLAZO:** *Para la falta de políticas:* • Especificar los activos importantes para el sistema de información académica. • Asignar responsabilidades sobre cada activo a los diferentes cargos y usuarios. • Definir el nivel de seguridad que debe tener cada activo del sistema de información académica. • Clasificar la información manejada dentro del sistema de información académica (nivel de confidencialidad). • Especificar el manejo que se debe dar a cada activo del sistema de información académica según su nivel de seguridad • Especificar las sanciones a aplicar

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			cada vez que se presente un incidente de seguridad determinado. • Determinar si las políticas de seguridad establecidas van en concordancia con las leyes de protección de datos personales y de seguridad informática vigentes a nivel nacional. Si no es así, realizar los ajustes necesarios. • Determinar si las políticas de seguridad establecidas van en concordancia con las políticas de seguridad institucionales. Si no es así, realizar los ajustes necesarios. • Obtener la aprobación de las políticas del sistema de información académica por parte de las directivas de la institución *Para la falta de capacitación y concientización:* • Identificar los errores comunes que cometen los **administrativos** al manejar el sistema de información académica, y que colocan en riesgo la información almacenada en él. • Definir los objetivos del programa de concientización • Establecer la estructura del programa de concientización, definiendo las diferentes fases que lo conformarán. Se debe tener en cuenta que dicha concientización debe realizarse desde el momento en que la persona entra a hacer parte de la institución y luego realizar periódicamente actividades que refuercen y actualicen lo aprendido. • Obtener la aprobación y financiamiento del programa por parte de las directivas de la

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			institución • Seleccionar los temas que se van a abordar durante la concientización. Entre los temas a tener en cuenta están: leyes de delitos informáticos y de protección de datos personales, importancia del rol de los **Administrativos** en la cadena de seguridad, precauciones que se deben tener antes de acceder al sistema de información acádemica, medidas de seguridad que se deben tener en cuenta mientras se esté consultando el sistema, medidas de seguridad que se deben tener con la información que se descarga o sube al sistema, características mínimas que debe tener la contraseña de acceso al sistema de información académica para que sea segura. • Definir las estrategias y actividades a llevar a cabo para desarrollar los diferentes temas del programa • Elaborar el material que se utilizará en las actividades de concientización • Entrenar al personal que se encargará de realizar la concientización **A LARGO PLAZO** *Para la falta de políticas:* • Realizar revisiones periódicas de las políticas de seguridad del sistema de información académica, de manera que sean adecuadas para el contexto interno como externo de la institución

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			Para la falta de capacitación y concientización: • Realizar las actividades de concientización planteadas • Entregar el material elaborado para las diferentes actividades (posters, boletines, etc.) • Monitorear el programa de concientización • Documentar y evaluar los resultados del programa de concientización • Realizar los cambios que se crean pertinentes al programa de concientización
Centro de Datos Donde Están el Servidor de Base de Datos de Información Académica y el de Autenticación	**20**	Falta de plan de contingencia	**A CORTO PLAZO:** • Elaborar plan de contingencia para el **centro de datos**, a fin de saber cómo actuar ante incidentes o fallas inesperados. **A LARGO PLAZO:** • Revisar el plan de contingencia periódicamente para realizar mejoras • Dar a conocer el plan de contingencia al personal del CIADTI encargado del **centro de datos**
Docentes	**21**	Almacenamiento desprotegido de la información que se descarga y sube al campus TI	**A CORTO PLAZO:** • Tener copias de respaldo cifradas de la información • Guardar la información de manera cifrada • Mantener vigilado el medio de almacenamiento de la información, para que no caiga en manos indeseadas **A LARGO PLAZO:** • Verificar la integridad de la información almacenada cuando

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			sea necesario • Utilizar las copias de respaldo para recuperar la información en caso de algún daño
Docentes	**22**	Ingreso al sistema de información académica desde sitios públicos y falta de precauciones de seguridad al ingresar al campus	**A CORTO PLAZO:** *Para el ingreso desde sitios públicos:* • Tomar precauciones de seguridad al ingresar al sistema, para no exponer la contraseña de acceso y evitar fisgones. • No olvidar cerrar la sesión del sistema de información académica. • Borrar rastros de navegación del computador antes de irse *Para la falta de precauciones:* • Realizar jornadas de concientización y capacitación a los **docentes** sobre el uso adecuado del sistema de información académica (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad). **A LARGO PLAZO:** *Para el ingreso desde sitios públicos:* • Buscar un sitio que brinde mejores condiciones de seguridad para ingresar al sistema de información académica

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Servicio de Autenticación al Campus TI	**23**	Falta de mecanismo de autenticación fuerte, uso de contraseñas débiles por parte de los usuarios, y ausencia de límite de intentos de autenticación	**A CORTO PLAZO:** • Habilitar las directivas de las contraseñas para que se emplee un conjunto amplio de caracteres (mayúsculas, minúsculas, números, símbolos), que la contraseña tenga un número mínimo de caracteres, que haya un historial de contraseñas, que se deba cambiar la contraseña después de un número determinado de días y que se bloqueen las cuentas después de un número determinado de intentos fallidos. **A LARGO PLAZO:** • Implementar un mecanismo de autenticación fuerte para ingresar al sistema de información académica, que involucre al menos dos factores (algo que se conoce, algo que se posee, algo que se es). • Monitorear el mecanismo de autenticación • Analizar los datos arrojados por el monitoreo del mecanismo de autenticación, a fin de determinar su efectividad
Servicio de Autenticación al Campus TI	**24**	Fallas en el diseño e implementación del software que crean agujeros de seguridad	**A CORTO PLAZO:** • Informar a los desarrolladores sobre las fallas encontradas **A LARGO PLAZO:** • Cuando se le vaya a hacer alguna modificación al **servicio de autenticación** se debe usar una metodología de diseño de software que tenga en cuenta la seguridad y que posibilite realizar una buena documentación de los cambios realizados.

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Políticas del Sistema de Información Académica	**25**	Falta de divulgación de las políticas de seguridad del sistema de información académica	**A CORTO PLAZO:** • Asignar la responsabilidad de la creación e implementación de las estrategias de difusión a un cargo o área específica. • Establecer qué políticas de seguridad aplican a cada grupo de usuarios. • Definir la estrategia de difusión de las políticas de seguridad a cada grupo de usuarios. • Obtener la aprobación y financiamiento de las estrategias de difusión por parte de las directivas de la institución • Elaborar el material que se utilizará para difundir las políticas **A LARGO PLAZO:** • Dar a conocer las políticas de seguridad a cada grupo de usuarios • Monitorear las estrategias de difusión • Documentar y evaluar los resultados de las estrategias de difusión • Realizar los cambios que se crean pertinentes en las estrategias de difusión
Lugar desde Donde Consultan los Usuarios ACADEMUSOFT (Café internet, Domicilio, Universidad)	**26**	Falta de control de acceso y seguridad física en los sitios públicos	**A CORTO PLAZO:** • Tomar precauciones de seguridad al ingresar al sistema, para no exponer la contraseña de acceso y evitar fisgones. • No olvidar cerrar la sesión del sistema de información académica. • Borrar rastros de navegación del computador antes de irse. **A LARGO PLAZO:** • Buscar un sitio que brinde mejores condiciones de seguridad para ingresar al sistema de información

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			académica
Servidor de Base de Datos de Información Académica y de Autenticación	**27**	Falta de condiciones de refrigeración adecuadas.	**A CORTO PLAZO:** • Revisar si los ventiladores del **servidor** están funcionando adecuadamente, y si no es así, realizar la limpieza de los mismos o ver si se trata de un error en la conexión. **A LARGO PLAZO:** • Colocar aire acondicionado en el sitio donde se encuentra el **servidor**
Personal del CIADTI	**28**	Ausencia de auditorías (supervisiones) regulares de los empleados y su trabajo	**A CORTO PLAZO:** • Establecer los objetivos, alcance, criterios y frecuencia de las auditorías que se deben realizar a al **personal del CIADTI** a cargo de los activos del sistema de información académica (ver Falta de programa de auditorías del sistema de información académica). **A LARGO PLAZO:** • Realizar auditorías periódicas del **personal del CIADTI** y su trabajo (ver Falta de programa de auditorías del sistema de información académica).
Administrativos	**29**	Procedimientos inadecuados de contratación	**A CORTO PLAZO:** • Redefinir los pasos que se deben llevar a cabo para la contratación de los **Administrativos** • Definir correctamente los perfiles de las personas a contratar, en cuanto a conocimientos y cualidades humanas que deben tener. **A LARGO PLAZO:** • Realizar las entrevistas y las pruebas necesarias para verificar

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			que los candidatos cumplen con los perfiles establecidos • Capacitar adecuadamente al nuevo personal **Administrativo** antes de que empiece a desempeñar su cargo.
Administrativos	**30**	Ausencia de auditorías (supervisiones) regulares de los empleados y su trabajo	**A CORTO PLAZO:** • Establecer los objetivos, alcance, criterios y frecuencia de las auditorías que se deben realizar a a los **Administrativos** a cargo de los activos del sistema de información académica (ver Falta de programa de auditorías del sistema de información académica) **A LARGO PLAZO:** • Realizar auditorías periódicas a los **Administrativos** y su trabajo (ver Falta de programa de auditorías del sistema de información académica).
Imagen y Reputación de la Institución	**31**	Dar percepción errónea de seguridad a los usuarios del campus TI	**A CORTO PLAZO:** • Explicar adecuamente a los usuarios, desde la primera vez que ingresen al sistema, cómo funcionan las medidas de seguridad implantadas y qué rol juegan ellos en la cadena de la seguridad.
Dispositivos de almacenamiento de información de los usuarios (USB, Tablets, Teléfonos Móviles, etc.)	**32**	Ingreso de dispositivos en equipos no protegidos	**A CORTO PLAZO:** • Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre la seguridad que debe darse a la información que consultan y descargan del sistema (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			Seguridad)
Dispositivos Utilizados por los Usuarios para Acceder a ACADEMUSOFT (Teléfonos Móviles, PCs, Portátiles, etc.)	**33**	Descarga descontrolada e instalación de software libre	**A CORTO PLAZO:** • Crear cuentas de usuario en el equipo, de manera que exista un solo administrador, quien será el único con permisos para instalar programas. Para conectarse a Internet, deberán usarse las cuentas de usuario estándar o de invitado, nunca la cuenta de administrador. • Instalar un buen antivirus en el equipo • Actualizar diariamente el antivirus • Instalar y configurar adecuadamente un *firewall* de aplicación en el equipo • Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre las medidas de seguridad a tener en cuenta en los equipos (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Navegador WEB de los Usuarios	**34**	Instalación y activación indiscriminada de complementos	**A CORTO PLAZO:** • Realizar jornadas de concientización y capacitación a los usuarios sobre el uso adecuado del sistema de información académica (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Base de Datos de Información Académica (ACADEMUSOFT)	**35**	Almacenamiento sin la debida protección de la información académica	**A CORTO PLAZO:** • Tener copias de respaldo de la información de la **Base de Datos** • Guardar la información de la **Base de Datos** de manera cifrada • Mantener vigilado el servidor de la **Base de Datos**, para que la información no caiga en manos indeseadas **A LARGO PLAZO:** • Verificar la integridad de la información en la **Base de Datos** almacenada cuando sea necesario • Utilizar las copias de respaldo para recuperar la información de la **Base de Datos** en caso de algún daño
Base de Datos de Información Académica (ACADEMUSOFT)	**36**	Falta de copias de respaldo.	**A CORTO PLAZO:** • Realizar diariamente copias de respaldo de la información de la **Base de Datos** **A LARGO PLAZO:** • Utilizar las copias de respaldo para recuperar la información de la **Base de Datos** en caso de algún daño
Base de Datos de Información Académica (ACADEMUSOFT)	**37**	Especificaciones incompletas o no claras para los desarrolladores	**A CORTO PLAZO:** • Elaborar o completar la documentación de la **Base de Datos de Información Académica**, de manera que sea comprensible para los desarrolladores **A LARGO PLAZO:** • Cuando se le vaya a hacer alguna modificación al software de la **Base de Datos de Información Académica** se debe usar una metodología de diseño de software que tenga en cuenta la

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			seguridad y que posibilite realizar una buena documentación de los cambios realizados.
Base de Datos de Información Académica (ACADEMUSOFT	**38**	Falta de mecanismo de autenticación fuerte	**A CORTO PLAZO:** • Habilitar las directivas de las contraseñas para que se emplee un conjunto amplio de caracteres (mayúsculas, minúsculas, números, símbolos), que la contraseña tenga un número mínimo de caracteres, que haya un historial de contraseñas, que se deba cambiar la contraseña después de un número determinado de días y que se bloqueen las cuentas después de un número determinado de intentos fallidos. **A LARGO PLAZO:** • Implementar un mecanismo de autenticación fuerte para ingresar al sistema de información académica, que involucre al menos dos factores (algo que se conoce, algo que se posee, algo que se es). • Monitorear el mecanismo de autenticación • Analizar los datos arrojados por el monitoreo del mecanismo de autenticación, a fin de determinar su efectividad
Servidor de Base de Datos de Información Académica y de Autenticación	**39**	Falta de realización periódica de copias de respaldo	**A CORTO PLAZO:** • Realizar diariamente copias de respaldo de la información del **Servidor de Base de Datos de Información Académica y de Autenticación** **A LARGO PLAZO:** • Utilizar las copias de respaldo para recuperar la información en caso

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			de algún daño en el **Servidor de Base de Datos de Información Académica y de Autenticación**
Servidor de Base de Datos de Información Académica y de Autenticación	**40**	Ausencia de esquemas de reemplazo periódico	**A CORTO PLAZO:** • Planear el reemplazo periódico del **Servidor de Base de Datos de Información Académica y de Autenticación.** **A LARGO PLAZO:** • Realizar el reemplazo **del Servidor de Base de Datos de Información Académica y de Autenticación** según el esquema de reemplazo periódico
Servidor de Base de Datos de Información Académica y de Autenticación	**41**	Ausencia de revisión periódica de las bitácoras (logs) del servidor y de monitoreo del sistema en busca de fallas e incidentes de seguridad	**A CORTO PLAZO:** • Revisar diariamente los logs (bitácoras) del **Servidor de Base de Datos de Información Académica y de Autenticación**, para detectar posibles fallos que se estén presentando.
Centro de Datos Donde Están el Servidor de Base de Datos de Información Académica y el de Autenticación	**42**	Falta de control de acceso al centro de datos.	**A CORTO PLAZO:** • Colocar rejas de seguridad en las ventanas • Ubicar los equipos de manera que no queden cerca a las ventanas • Controlar el acceso al **centro de datos**, de manera que sólo personas autorizadas puedan acceder a él **A LARGO PLAZO:** • Verificar la efectividad de cada una de las medidas de seguridad física implementadas y realizar los cambios que se consideren necesarios • Instalar un sistema de videovigilancia para visualizar quienes ingresan al **centro de datos**

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Centro de Datos Donde Están el Servidor de Base de Datos de Información Académica y el de Autenticación	**43**	Presencia de humedad, polvo y suciedad.	**A CORTO PLAZO:** • Verificar que el **centro de datos** no tiene filtraciones o algún tipo de humedad que pueda afectar los equipos **A LARGO PLAZO:** • Realizar con frecuencia una limpieza adecuada del **centro de datos**
Imagen y Reputación de la Institución	**44**	Corrupción	**A CORTO PLAZO:** • Realizar auditorías periódicas a los empleados y su trabajo (ver Falta de programa de auditorías del sistema de información académica) • Aplicar sanciones establecidas a las personas que no hacen correctamente su trabajo **A LARGO PLAZO:** • Realizar jornadas de concientización a los empleados, indicando las sanciones que trae el hacer mal uso de los activos del sistema de información académica (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad).
Políticas del Sistema de Información Académica	**45**	Ausencia de procedimientos de identificación y valoración de riesgos	**A CORTO PLAZO:** • Elaborar procedimientos de identificación, valoración y análisis de riesgos. **A LARGO PLAZO:** • Ejecutar los procedimientos de identificación, valoración y análisis de riesgos para identificar los riesgos todavía presentes en el sistema.

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Dispositivos Utilizados por los Usuarios para Acceder a ACADEMUSOFT (Teléfonos Móviles, PCs, Portátiles, etc.)	**46**	Ausencia de terminación de sesión cuando se abandona la estación de trabajo	**A CORTO PLAZO:** • Configurar el equipo para que se bloquee automáticamente mínimo después de un minuto de inactividad y que solicite la contraseña para desbloquearse. • Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre las medidas de seguridad a tener en cuenta en los equipos (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Administrativos	**47**	Falta de personal suficiente y sobrecarga de trabajo del personal existente	**A CORTO PLAZO:** • Definir correctamente los perfiles de las personas a contratar, en cuanto a conocimientos y cualidades humanas que deben tener. • Realizar la selección, contratación y capacitación de personal en las áreas con sobrecarga de trabajo **A LARGO PLAZO:** • Revisar las funciones de cada cargo y determinar si estas funciones deben ser redistribuidas de manera más equitativa para evitar sobrecargas • Realizar los cambios pertinentes en la definición de funciones de los cargos
Estudiantes	**48**	Ingreso al sistema de información académica desde sitios públicos y falta de precauciones de seguridad al ingresar al campus	**A CORTO PLAZO:** *Para el ingreso desde sitios públicos:* • Tomar precauciones de seguridad al ingresar al sistema, para no exponer la contraseña de acceso y evitar fisgones. • No olvidar cerrar la sesión del sistema de información académica. • Borrar rastros de navegación del

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			computador antes de irse *Para la falta de precauciones:* • Realizar jornadas de concientización y capacitación a los **estudiantes** sobre el uso adecuado del sistema de información académica (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad). **A LARGO PLAZO:** *Para el ingreso desde sitios públicos:* • Buscar un sitio que brinde mejores condiciones de seguridad para ingresar al sistema de información académica
Dispositivos de Almacenamiento de Información de los Usuarios (USB, Tablets, Teléfonos Móviles, etc.)	**49**	Descuido del lugar donde se dejan los dispositivos	**A CORTO PLAZO:** • Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre la seguridad que debe darse a la información que consultan y descargan del sistema (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Dispositivos Utilizados por los Usuarios para Acceder a ACADEMUSOFT (Teléfonos Móviles, PCs, Portátiles, etc.)	**50**	Uso compartido del dispositivo.	**A CORTO PLAZO:** • Crear cuentas de usuario en el equipo, de manera que exista un solo administrador, quien será el único con permisos para instalar programas. Para conectarse a Internet, deberán usarse las cuentas de usuario estándar o de invitado, nunca la cuenta de administrador. • Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre las

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			medidas de seguridad a tener en cuenta en los equipos (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Base de Datos de Información Académica (ACADEMUSOFT)	**51**	Interfaz de usuario compleja	**A CORTO PLAZO:** • Capacitar a los usuarios sobre el uso adecuado de la aplicación y de las ayudas que posee **A LARGO PLAZO:** • Elaborar un manual de usuario de la aplicación más específico, preguntar a los usuarios sobre las dificultades que encuentran en el uso de la interfaz y realizar los cambios necesarios a fin de reducir su complejidad
Servidor de Base de Datos de Información Académica y de Autenticación	**52**	Falta de puntos de restauración del sistema	**A CORTO PLAZO:** • Insertar puntos de restauración en el sistema cada vez que se realicen cambios en la instalación o configuración del **servidor** **A LARGO PLAZO:** • Restaurar el sistema en caso de algún daño en el sistema operativo
Servidor de Base de Datos de Información Académica y de Autenticación	**53**	Susceptibilidad a la humedad, el polvo y la suciedad.	**A CORTO PLAZO:** • Verificar que el centro de datos no tiene filtraciones o algún tipo de humedad que pueda afectar el **servidor** **A LARGO PLAZO:** • Realizar con frecuencia una limpieza adecuada del lugar donde se encuentra el **servidor**

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Canal de Comunicación Cliente/Servidor	**54**	Gestión inadecuada de la red	**A CORTO PLAZO:** • Contratar el ancho de banda necesario para el sistema de información académica, según el volumen de tráfico que este maneja **A LARGO PLAZO:** • Monitorear constantemente los servidores, los dispositivos de red y los enlaces por donde se enruta el tráfico del sistema de información académica, a través de un servidor SNMP. • Analizar la información entregada por el servidor SNMP y sacar estadísticas. • Realizar los cambios que se consideren necesarios en los servidores y en la red para solucionar los problemas que se presentan.
Navegador WEB de los usuarios	**55**	Ausencia de terminación de sesión cuando se abandona la estación de trabajo	**A CORTO PLAZO:** • Configurar los servicios para que las sesiones de los usuarios se terminen después de varios minutos de inactividad. • Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre las medidas de seguridad a tener en cuenta en los equipos (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Estudiantes	**56**	Falta de confidencialidad de la información que descarga del sistema de información académica	**A CORTO PLAZO:** • Realizar jornadas de concientización y capacitación a los **estudiantes** sobre la seguridad que debe darse a la información que consultan y descargan del sistema de información académica

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			(ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad) • Guardar la información de manera cifrada • Mantener vigilado el medio de almacenamiento de la información, para que no caiga en manos indeseadas
Políticas del Sistema de Información Académica	**57**	Ausencia de procedimiento formal para el control de la documentación del SGSI	**A CORTO PLAZO:** • Definir un procedimiento formal para el control de la documentación del SGSI **A LARGO PLAZO:** • Aplicar el procedimiento establecido y documentar adecuadamente el SGSI
Base de Datos de Información Académica (ACADEMUSOFT)	**58**	Ausencia de control de cambios eficaz, que permite otorgar privilegios de manera indiscriminada a ciertos usuarios y falta de roles definidos para los diferentes tipos de usuarios	**A CORTO PLAZO:** • Establecer los procedimientos de asignación y retiro de privilegios de acceso al sistema de información académica, de los diferentes tipos de usuarios. • Definir procedimientos formales para la revisión periódica (supervisión) de los derechos de acceso al sistema de información académica de cada usuario. **A LARGO PLAZO:** • Revisar periódicamente los derechos de acceso al sistema de información académica de cada usuario
Servidor de Base de Datos de Información Académica y de Autenticación	**59**	Falta de control de los cambios hechos en la configuración del servidor	**A LARGO PLAZO:** • Documentar adecuadamente los cambios en la configuración que se le realicen al servidor

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Servidor de Base de Datos de Información Académica y de Autenticación	**60**	Falta de contraseña robusta de administrador	**A CORTO PLAZO:** • Configurar contraseñas seguras para cada una de las cuentas de usuario. Se recomienda que la contraseña de la cuenta de administrador sólo la conozca una sola persona. **A LARGO PLAZO:** • Cambiar periódicamente la contraseña de administrador por una contraseña que cumpla las características mínimas de seguridad
Servidor de Base de Datos de Información Académica y de Autenticación	**61**	Ausencia de terminación de sesión cuando se abandona el servidor	**A CORTO PLAZO:** • Configurar el **servidor** para que se bloquee automáticamente, mínimo después de un minuto de inactividad, y que solicite la contraseña para desbloquearse. • Realizar jornadas de concientización y capacitación al personal del CIADTI sobre las medidas de seguridad a tener en cuenta en el **servidor** (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Servidor de Base de Datos de Información Académica y de Autenticación	**62**	Acceso de múltiples personas al servidor	• Crear cuentas de usuario en el **servidor**, de administrador y usuarios estándar. Se debe limitar el número de personas con permisos de acceso al **servidor** al mínimo. • Realizar jornadas de concientización y capacitación al personal del CIADTI sobre las medidas de seguridad a tener en cuenta en el **servidor** (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad)
Centro de Datos Donde Están el	**63**	Ubicación en un área susceptible a inundación y	**A CORTO PLAZO:** • Ubicar el **centro de datos** en un área que no sea susceptible a

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Servidor de Base de Datos de Información Académica y el de Autenticación		desastres naturales	desastres naturales.
Servicio de Autenticación al Campus TI	**64**	Almacenamiento en claro de las contraseñas (tablas de contraseñas sin protección)	**A CORTO PLAZO:** • Guardar las contraseñas de los usuarios de manera cifrada en la base de datos
Canal de Comunicación Cliente/Servidor	**65**	Conexiones a red pública sin protección	**A CORTO PLAZO:** • Instalar un *firewall* en el perímetro de la red • Determinar las reglas que se deben configurar para controlar el tráfico entrante y saliente de la red institucional • Configurar correctamente en el *firewall*, las reglas de control de tráfico establecidas • Instalar y configurar un sistema de detección de intrusos (IDS) integrado con el *firewall*. • Instalar y configurar un servidor SNMP que permita monitorear el enlace con el ISP (Proveedor de Servicios de Internet) y el *firewall* **A LARGO PLAZO:** • Monitorear constantemente el tráfico del enlace con el ISP y el *firewall*. • Revisar constantemente los logs (bitácoras) del servidor SNMP • Analizar la información entregada por el servidor SNMP y sacar estadísticas • Verificar periódicamente la efectividad del *firewall* y del IDS • Realizar los cambios en la configuración del *firewall*, del IDS y del servidor SNMP que se consideren necesarios.

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
Base de Datos de Información Académica (ACADEMUSOFT)	**66**	Información viajando en claro por la red.	**A CORTO PLAZO:** • Cifrar la información mientras viaja por la red, a través de algún protocolo seguro, como SSL/TLS.
Servidor de Base de Datos de Información Académica y de Autenticación	**67**	Copia no controlada de la información del servidor	**A CORTO PLAZO:** • Almacenar las copias de respaldo de la información en un lugar seguro y de manera ordenada • Limitar el número de personas con permisos de acceso al servidor y sus copias de respaldo
Centro de Datos Donde Están el Servidor de Base de Datos de Información Académica y el de Autenticación	**68**	Falta de aire acondicionado	**A CORTO PLAZO:** • Colocar aire acondicionado en el **centro de datos** **A LARGO PLAZO:** • Realizar mantenimiento periódico al aire acondicionado
Servicio de Autenticación al Campus TI	**69**	Usuario y contraseña viajando en claro por la red	**A CORTO PLAZO:** • Cifrar la información mientras viaja por la red, a través de algún protocolo seguro, como SSL/TLS.
Servicio de Autenticación al Campus TI	**70**	Interfaz de usuario compleja que causa demora en el ingreso al campus y solicitud de ayuda para ingresar	**A CORTO PLAZO:** • Capacitar a los usuarios sobre el uso adecuado de la aplicación y de las ayudas que posee **A LARGO PLAZO:** • Elaborar un manual de usuario de la aplicación más específico, preguntar a los usuarios sobre las dificultades que encuentran en el uso de la interfaz y realizar los cambios necesarios a fin de reducir su complejidad
Navegador WEB de los Usuarios	**71**	Falta de configuración del navegador en cuanto a: bloqueo de cookies, almacenamiento de contraseñas, nivel de seguridad, almacenamiento	**A CORTO PLAZO:** • Realizar jornadas de concientización y capacitación a los usuarios sobre el uso adecuado del sistema de información académica (ver en Tabla 11 y Tabla 12 Falta de

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
		de historial, etc.	Capacitación y Concientización en Seguridad)
Dispositivos Utilizados por los Usuarios para Acceder a ACADEMUSOFT (Teléfonos Móviles, PCs, Portátiles, etc.)	**72**	Mantenimiento insuficiente.	**A CORTO PLAZO:** • Realizar jornadas de concientización y capacitación a los usuarios del sistema de información académica sobre las medidas de seguridad a tener en cuenta en los equipos (ver en Tabla 11 y Tabla 12 Falta de Capacitación y Concientización en Seguridad) **A LARGO PLAZO:** • Realizar periódicamente mantenimiento de software y hardware al equipo
Navegador WEB de los usuarios	**73**	Desbordamiento de Buffer	**A CORTO PLAZO:** • Actualizar el navegador o cambiarlo por otro
Servidor de Base de Datos de Información Académica y de Autenticación	**74**	Sensibilidad a la radiación electromagnética.	**A CORTO PLAZO:** • Ubicar el **servidor** en un lugar donde no ocurran radiaciones electromagnéticas fuertes
Dispositivos de Almacenamiento de Información de los Usuarios (USB, Tablets, Teléfonos Móviles, etc.)	**75**	Susceptibilidad a la humedad, el polvo y la suciedad.	**A CORTO PLAZO:** • Verificar que el lugar donde se encuentran los **dispositivos** no tiene filtraciones o algún tipo de humedad que pueda afectarlos **A LARGO PLAZO:** • Realizar con frecuencia una limpieza adecuada del lugar donde se encuentran los dispositivos
Dispositivos de Almacenamiento de Información de los Usuarios (USB, Tablets, Teléfonos Móviles, etc.)	**76**	Ausencia de copias de respaldo	**A CORTO PLAZO:** • Realizar diariamente copias de respaldo de la información importante **A LARGO PLAZO:** • Utilizar las copias de respaldo para recuperar la información en caso

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
			de algún daño
Lugar desde Donde Consultan los Usuarios ACADEMUSOFT (Café Internet, Domicilio, Universidad)	**77**	Red eléctrica inestable	**A CORTO PLAZO:** • Verificar que la instalación eléctrica del lugar donde se encuentran los equipos cuenta con la suficiente potencia y está en óptimas condiciones para soportarlos todos • Conectar los equipos a través de un regulador a la red eléctrica • Adquirir UPSs para los equipos, a fin que no salgan de funcionamiento cuando hayan cortes de energía **A LARGO PLAZO:** • Realizar mantenimiento periódico a la instalación eléctrica del lugar donde se encuentran los equipos
Dispositivos Utilizados por los Usuarios para Acceder a ACADEMUSOFT (Teléfonos Móviles, PCs, Portátiles, etc.)	**78**	Susceptibilidad a la humedad, el polvo y la suciedad.	**A CORTO PLAZO:** • Verificar que el lugar donde se encuentran los **dispositivos** no tiene filtraciones o algún tipo de humedad que pueda afectarlos **A LARGO PLAZO:** • Realizar con frecuencia una limpieza adecuada del lugar donde se encuentran los **dispositivos**
Dispositivos de Almacenamiento de Información de los Usuarios (USB, Tablets, Teléfonos Móviles, etc.)	**79**	Sensibilidad a la radiación electromagnética.	**A CORTO PLAZO:** • Ubicar los **dispositivos** en un lugar donde no ocurran radiaciones electromagnéticas fuertes
Dispositivos Utilizados por los Usuarios para Acceder a ACADEMUSOFT	**80**	Sensibilidad a la radiación electromagnética	**A CORTO PLAZO:** • Ubicar los **dispositivos** en un lugar donde no ocurran radiaciones electromagnéticas fuertes

ACTIVO	PRIORIZACIÓN	VULNERABILIDAD	CONTROLES
(Teléfonos Móviles, PCs, Portátiles, etc.)			

7 VALIDACIÓN DE LA METODOLOGÍA DE PREVENCIÓN DE RIESGOS PARA SISTEMAS DE INFORMACIÓN ACADÉMICA (MEPRISIA)

La validación de la metodología MePRiSIA se realizó teniendo en cuenta los aspectos considerados al diseñarla, es decir, según el análisis hecho a las metodologías existentes, se pudo concluir que la definición de estas metodologías es bastante compleja y que no todas incluían el factor humano en cada uno de sus pasos. Además, la complejidad propia de dichas metodologías las hacía difíciles de implementar. Por tanto, lo que se le pidió a los expertos fue que evaluaran si cada uno de los cuatro pasos de MePRiSIA son fáciles de entender, incluyen el factor humano y son fáciles de implementar.

Se utilizó el método de consenso Delphi para el análisis de los resultados obtenidos. El proceso de validación se compone de los pasos mostrados en la Figura 13, según lo estipulado en .

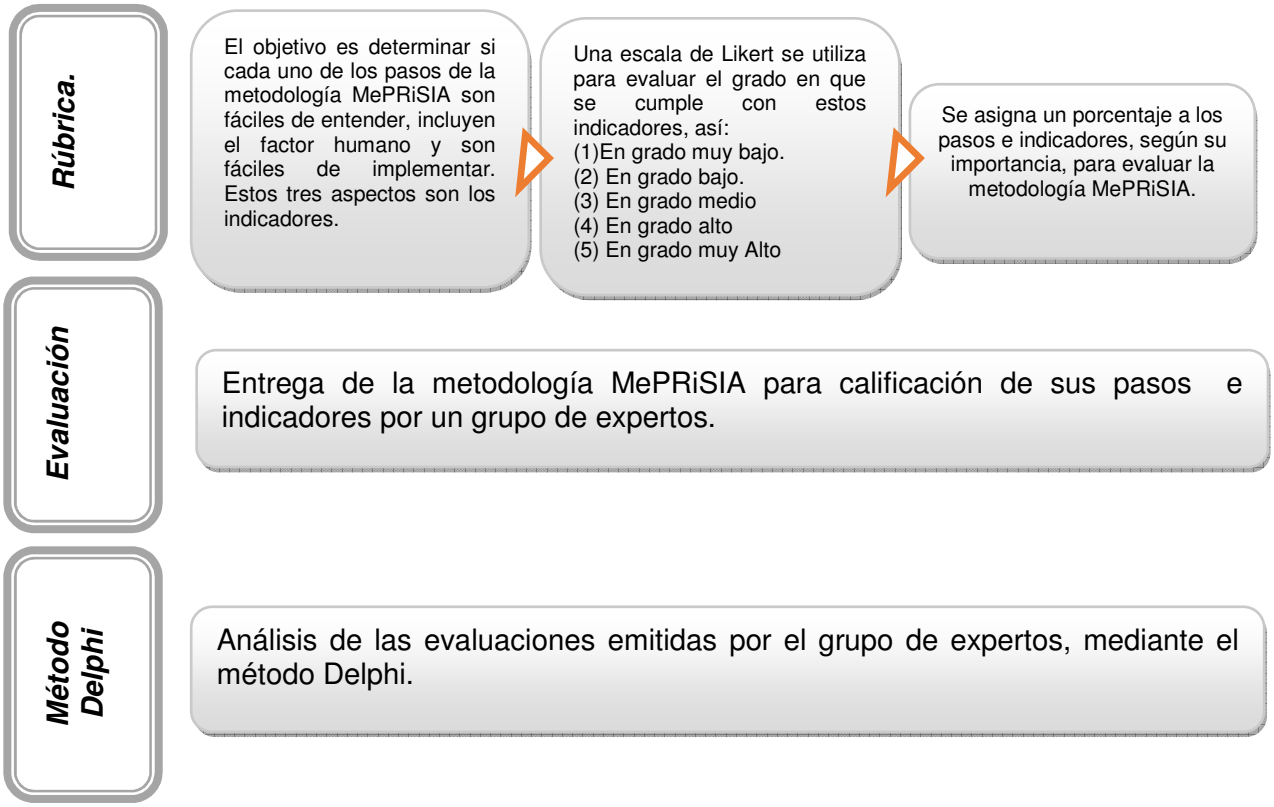

Figura 13: Proceso de Validación de la Metodología MePRiSIA.
Fuente: *Elaboración Propia*

7.1 RÚBRICA

Para : “las rúbricas son guías que valoran los aprendizajes y productos realizados”. Por ello, en el presente trabajo, se utilizó una rúbrica para evaluar los pasos de la metodología MePRiSIA, con base en tres indicadores:

- Fácil de Entender
- Incluye el factor Humano
- Fácil de Implementar

En la Figura 14 se muestra la rúbrica elaborada para la validación de la metodología por parte de los expertos.

RÚBRICA PARA EVALUACIÓN DE LA METODOLOGÍA DE PREVENCIÓN DE RIESGOS PARA SISTEMAS DE INFORMACIÓN ACADÉMICA (MePRISIA)

Nombre del Experto: _____

De acuerdo a la siguiente escala de Likert, determine el grado de claridad, inclusión del factor humano y facilidad de implementación de cada uno de los pasos de la Metodología de Prevención de Riesgos para Sistemas de Información Académica (MePRISIA):

- 1: En grado muy bajo
- 2: En grado bajo
- 3: En grado medio
- 4: En grado alto
- 5: En grado muy alto

PASOS	Fácil de Entender	Incluye el Factor Humano	Fácil de Implementar	OBSERVACIONES
Paso 1: Establecimiento del Contexto.				
Paso 2: Identificación de Riesgos				
Paso 3: Análisis de Riesgos				
Paso 4: Prevención de Riesgos				

Firma del Experto: _____

Figura 14. Rúbrica para la Evaluación de la Metodología

7.1.1 PONDERACIÓN DE LOS PASOS E INDICADORES

En la Tabla 34 se muestra el porcentaje dado a cada uno de los pasos e indicadores, según su grado de importancia para la metodología. Al primer paso se le asigna un peso porcentual del 20%, al segundo y tercer paso se les asigna el 25%, y al cuarto paso se le asigna el 30%, ya que se trata de una metodología de prevención de riesgos.

Tabla 34: Matriz de Ponderación de los Pasos e Indicadores de MePRiSIA.
Fuente: Basado en Modelo para la Gestión de Comunicaciones en Proyectos de Telecomunicaciones

PONDERACIÓN DE PASOS E INDICADORES PARA LA EVALUACIÓN DE LA METODOLOGÍA MePRISIA.		
PASOS E INDICADORES	**PONDERACIÓN**	**JUSTIFICACIÓN**
PASO 1: Establecimiento del Contexto	20%	A este paso se le asignó el 20% porque la información obtenida en este paso sirve como base para desarrollar los demás pasos de la metodología.
Fácil de Entender	8%	A este indicador se le asignó la ponderación más alta (8%), ya que en este paso se obtiene la información que sirve como base para desarrollar los demás pasos, así que es necesario que sea lo suficientemente claro como para que las personas que llevan a cabo la metodología entiendan fácilmente qué información deben obtener del sistema de información académica y sus usuarios.
Incluye el Factor Humano	7%	A este indicador se le asignó el 7%, ya que las personas son el eslabón más débil en la cadena de seguridad, por lo que es necesario que sean considerados desde el primer paso de la metodología.
Fácil de Implementar	5%	A este indicador se le asignó la ponderación más baja (5%), ya que la implementación de este paso depende en gran medida de la información que esté dispuesta a proporcionar la institución y las personas encargadas de los activos. Además, no siempre las instituciones cuentan con toda la información requerida.
PASO 2: Identificación de Riesgos	25%	A este paso se le asignó el 25% porque de la identificación adecuada y completa de los riesgos van a depender en gran medida los controles preventivos a implementar.

PONDERACIÓN DE PASOS E INDICADORES PARA LA EVALUACIÓN DE LA METODOLOGÍA MePRISIA.		
PASOS E INDICADORES	**PONDERACIÓN**	**JUSTIFICACIÓN**
Fácil de Entender	10%	A este indicador se le asignó el 10%, ya que es importante que quién identifica los riesgos comprenda bien lo que se debe hacer en este paso para que valore adecuadamente los activos e identifique las vulnerabilidades y amenazas de estos.
Incluye el Factor Humano	10%	A este indicador se le asignó el 10%, ya que es importante tener muy en cuenta a las personas en esta identificación como activos y fuentes de amenazas y vulnerabilidades.
Fácil de Implementar	5%	A este indicador se le asignó el 5%, ya que la implementación de este paso depende en gran medida de la información que esté dispuesta a proporcionar la institución y las personas encargadas de los activos. Además, no siempre las instituciones cuentan con toda la información requerida, lo que puede llevar a inexactitudes en la identificación de los riesgos.
PASO 3: Análisis de Riesgos	25%	A este paso se le asignó el 25% porque es crucial para priorizar los diferentes riesgos que existen en el sistema de información académica.
Fácil de Entender	10%	A este indicador se le asignó el 10%, ya que es importante que quién valora los riesgos comprenda bien lo que se debe hacer en este paso para que la priorización de estos sea correcta.
Incluye el Factor Humano	10%	A este indicador se le asignó el 10%, ya que es importante tener en cuenta el punto de vista de los diferentes usuarios del sistema de información académica para determinar el impacto de los riesgos y su probabilidad de ocurrencia .
Fácil de Implementar	5%	A este indicador se le asignó el 5%, ya que la correcta implementación de este paso depende en gran medida de la información que brindó la institución y las personas encargadas de los activos en el paso anterior, que como dijimos puede estar incompleta o se inexacta.

PONDERACIÓN DE PASOS E INDICADORES PARA LA EVALUACIÓN DE LA METODOLOGÍA MePRISIA.		
PASOS E INDICADORES	**PONDERACIÓN**	**JUSTIFICACIÓN**
PASO 4: Prevención de Riesgos	30%	A este paso se le asignó el 30% porque al tratarse de una metodología de prevención de riesgos, es en este paso donde se realiza la labor de prevención a través de los diferentes controles propuestos.
Fácil de Entender	10%	A este indicador se le asignó el 10%, ya que es importante que quién priorizó los riesgos comprenda qué controles aplicar para prevenirlos o mitigarlos.
Incluye el Factor Humano	10%	A este indicador se le asignó el 10%, ya que el éxito de los controles a implementar depende en gran medida de que sean usados correctamente por los diferentes tipos de usuarios.
Fácil de Implementar	10%	A este indicador se le asignó el 10%, ya que de la elección adecuada de los controles dependerá la efectividad de la metodología.

7.2 EVALUACIÓN

7.2.1 GRUPO DE EXPERTOS

Para evaluar la Metodología MePRISIA, se eligieron dos expertos externos que cuentan con amplios conocimientos en seguridad informática y un experto interno conoce muy bien los sistemas de información académica. Su experiencia nos permite estar seguros que la evaluación y recomendaciones hechas a la metodología MePRiSIA son confiables.

En la Tabla 35 se presentan las características del grupo de expertos.

Tabla 35: Características de l Grupo de Expertos

Nombre	Profesión	Empresa	Área de desempeño	Experiencia
Rodrigo Alvear Tristancho	Ingeniero de Sistemas M.Sc. Gestión de Proyectos Informáticos	Universidad de Pamplona	Subdirector de Consultoría, y Coordinador Soporte Tecnológico.	10 años.
Rafael Vicente Páez Méndez	Ingeniero de Sistemas. Doctor en Ingeniería Telemática	Pontificia Universidad Javeriana-(Bogotá|	Profesor Asistente. Investigador Experto en Seguridad	9 años

Nombre	Profesión	Empresa	Área de desempeño	Experiencia
		Colombia)	Informática.	
Jordi Forné Muñoz	Doctor en Ingeniería en Telecomunicaciones.	Universidad Politécnica de Cataluña – (Barcelona – España)	Profesor Titular. Investigador Experto en Seguridad Informática	19 años

La rúbrica (Figura 14) y la metodología fueron enviadas vía correo electrónico a los expertos.

El proceso se realizó de manera confidencial para que no hubiera ninguna comunicación que dañara la objetividad del mismo.

7.2.2 EVALUACIONES

Las rúbricas diligenciadas por los expertos se muestran en la Figura 15, Figura 16, y Figura 17.

RÚBRICA PARA EVALUACIÖN DE LA
METODOLOGÍA DE PREVENCIÓN DE RIESGOS PARA SISTEMAS DE INFORMACIÓN ACADÉMICA (MePRiSIA)

Nombre del Experto: **RODRIGO ALVEAR TRISTANCHO**

De acuerdo a la siguiente escala de Likert, determine el grado de la claridad, inclusión del factor humano y facilidad de implementación de cada uno de los pasos de la Metodología de Prevención de Riesgos para Sistemas de Información Académica (MePRiSIA):

- 1: En grado muy bajo
- 2: En grado bajo
- 3: En grado medio
- 4: En grado alto
- 5: En grado muy alto

PASOS	*Fácil de Entender*	*Incluye el Factor Humano*	*Fácil de Implementar*	*OBSERVACIONES*
Paso 1: Establecimiento del Contexto.	5	5	2	Responder las preguntas del Paso 1 para muchas Instituciones de nuestro medio regional o nacional podría representar mucha dificultad pues por años le han restado importancia a los recursos de seguridad por lo que carecen de elementos y conocimiento para responder las preguntas en cuestión. Además, es notable la falta de interés de la alta dirección en las instituciones por los temas asociados a la prevención de riesgos, por lo cual llevar a cabo el simple Paso 1 va a requerir un gran esfuerzo y sensibilización por parte del experto de esta metodología.
Paso 2: Identificación de Riesgos	4	5	3	Luego de concluir el paso 1 y disponer de toda la información requerida en ese diagnóstico se estima que con el apoyo de un equipo de expertos, obviamente incluyendo personal de la entidad, se puede sacar adelante este paso.
Paso 3: Análisis de Riesgos	4	5	3	Al igual que el paso anterior, realizar el análisis de riesgos requiere de la participación de expertos en administración de riesgos y del personal experto de la entidad que haya evidenciado las situaciones identificadas.
Paso 4: Prevención de Riesgos	4	5	2	La prevención de los riesgos identificados requerirá hacer inversiones así como mucho compromiso del personal. En el medio en que vivimos, d...de los presupuestos de las entidades son limitados y, en algunos casos, se prioriza lo urgente, lo visible y lo inmediato, sobre la planeación y las acciones de resultado a largo plazo, va a requerirse un esfuerzo inmenso del equipo del proyecto que lleve a cabo la metodología para convencer a la alta dirección de la necesidad de las inversiones requeridas y sensibilizar al personal sobre la importancia de su participación activa para que la Institución evite situaciones que puedan destruirla.

Firma del Experto:

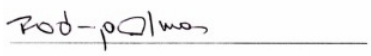

Figura 15. Rúbrica MSc Rodrigo Alvear

RÚBRICA PARA EVALUACIÖN DE LA
METODOLOGÍA DE PREVENCIÓN DE RIESGOS PARA SISTEMAS DE INFORMACIÓN ACADÉMICA (MePRiSIA)

Nombre del Experto: Rafael Vicente Páez Méndez

De acuerdo a la siguiente escala de Likert, determine el grado de la claridad, inclusión del factor humano y facilidad de implementación de cada uno de los pasos de la Metodología de Prevención de Riesgos para Sistemas de Información Académica (MePRiSIA):

- 1: En grado muy bajo
- 2: En grado bajo
- 3: En grado medio
- 4: En grado alto
- 5: En grado muy alto

PASOS	*Fácil de Entender*	*Incluye el Factor Humano*	*Fácil de Implementar*	*OBSERVACIONES*
Paso 1: Establecimiento del Contexto.	5	5	5	
Paso 2: Identificación de Riesgos	3	4	4	No es clara la utilidad de la Tabla para valoración de activos de personal ni cómo se evaluaría la Confidencialidad Integridad y Disponibilidad.
Paso 3: Análisis de Riesgos	5	5	5	
Paso 4: Prevención de Riesgos	5	5	5	

Firma del Experto:

Figura 16. Rúbrica PhD Rafael Páez

RÚBRICA PARA EVALUACIÖN DE LA
METODOLOGÍA DE PREVENCIÓN DE RIESGOS PARA SISTEMAS DE INFORMACIÓN ACADÉMICA (MePRiSIA)

Nombre del Experto: JORDI FORNÉ MUÑOZ

De acuerdo a la siguiente escala de Likert, determine el grado de la claridad, inclusión del factor humano y facilidad de implementación de cada uno de los pasos de la Metodología de Prevención de Riesgos para Sistemas de Información Académica (MePRiSIA):

- 1: En grado muy bajo
- 2: En grado bajo
- 3: En grado medio
- 4: En grado alto
- 5: En grado muy alto

PASOS	*Fácil de Entender*	*Incluye el Factor Humano*	*Fácil de Implementar*	*OBSERVACIONES*
Paso 1: Establecimiento del Contexto.	5	5	5	
Paso 2: Identificación de Riesgos	5	5	5	
Paso 3: Análisis de Riesgos	5	5	4	Se afirma que la escala de Likert presentada en la página 8 es exponencial. Para serlo en sentido estricto, si el primer intervalo es del 50%, el segundo debería ser exactamente del 25%, el tercero del 12.5% y así sucesivamente. Debería decirse una "escala no lineal", o a lo sumo "cuasi exponencial".
Paso 4: Prevención de Riesgos	5	5	4	Creo que sería adecuado añadir una breve sección de conclusiones para finalizar el documento.

Firma del Experto:

Figura 17. Rúbrica PhD Jordi Forné

7.3 MÉTODO DELPHI

El método Delphi es una herramienta que exige el consenso dentro de un grupo de expertos con respecto a un tema en particular. La investigadora lo define como: "uno de los métodos generales de prospectiva, que busca acercarse al consenso de un grupo de expertos con base en el análisis y la reflexión de un problema definido". Para la investigadora, el grupo de expertos debe asumir la responsabilidad de emitir juicios y opiniones, que son lo que constituye el eje del método. Dependiendo del grado de consenso, muchas veces podría ser necesario realizar varios sondeos para que al final se llegue a un consenso grupal.

7.3.1 MATRIZ DE RESULTADOS

La matriz de resultados que se observa en la Tabla 36**,** se compone de los siguientes campos:

1. **Pasos e Indicadores**: Contiene los pasos de la metodología y los indicadores que se evalúan.
2. **Calificación Experto X**: Es la calificación que dio cada uno de los expertos a cada indicador, de acuerdo a la escala de Likert establecida (1: En grado muy bajo, 2: En grado bajo, 3: En grado medio, 4: En grado alto, 5: En grado muy alto).

3. **Promedio del Consenso**: Es el promedio de las calificaciones dadas por los expertos a cada indicador.
4. **Variación Estándar**: Es la desviación estándar de cada indicador.
5. **Ponderación Asignada**: Es la ponderación asignada a cada paso e indicador, según lo establecido en la Tabla 34.
6. **Valor Alcanzado**: Se calcula multiplicando el promedio del consenso por la ponderación asignada, dividido por el máximo valor de la escala de Likert (5).
7. **Grado de Cumplimiento**: Se calcula multiplicando el Valor Alcanzado por 100 dividido entre la Ponderación Asignada. Además, se le dio un color, según la siguiente escala:

   0% - 69%= **BAJO**

   70% - 89%= **MEDIO**

   90% - 100%= **ALTO**

Además, se estableció que para que exista consenso, el margen de desviación de las calificaciones asignadas a cada indicador no debe ser mayor a 2.0. De no existir consenso en uno o varios indicadores se deberá ir a una segunda ronda.

Tabla 36: Matriz de Resultados
Fuente: Basado en Modelo para la Gestión de Comunicaciones en Proyectos de Telecomunicaciones

MATRIZ DE RESULTADOS METODOLOGÍA DE PREVENCIÓN DE RIESGOS PARA SISTEMAS DE INFORMACIÓN ACADÉMICA (MePRISIA) Primera Ronda								
PASOS E INDICADORES	**Calificación Experto 1**	**Calificación Experto 2**	**Calificación Experto 3**	**Promedio del Consenso**	**Variación Estándar**	**Ponderación Asignada**	**Valor Alcanzado**	**Grado de Cumplimiento**
PASO 1 : Establecimiento del contexto						**20%**	19%	95%
Fácil de Entender	5	5	5	5	0	**8%**	8%	100%
Incluye el Factor Humano	5	5	5	5	0	**7%**	7%	100%
Fácil de Implementar	2	5	5	4	1,73	**5%**	4%	80%
PASO 2 : Identificación de Riesgos						**25%**	21,33%	85,33%

Fácil de Entender	4	3	5	4	1	**10%**	8%	80%
Incluye el Factor Humano	5	4	5	4,67	0,58	**10%**	9,33%	93,33%
Fácil de Implementar	3	4	5	4	1	**5%**	4%	80%
PASO 3: Análisis de Riesgos.						**25%**	23,33%	93,33%
Fácil de Entender	4	5	5	4,67	0,58	**10%**	9,33%	93,33%
Incluye el Factor Humano	5	5	5	5	0	**10%**	10%	100%
Fácil de Implementar	3	5	4	4	1	**5%**	4%	80%
PASO 4 : Prevención de Riesgos						**30%**	26,67%	88,89%
Fácil de Entender	4	5	5	4,67	0,58	**10%**	9,33%	93,33%
Incluye el Factor Humano	5	5	5	5	0	**10%**	10%	100%
Fácil de Implementar	2	5	4	3,67	1,53	**10%**	7,33%	73,33%

7.3.2 ANÁLISIS DE RESULTADOS

Como se puede ver en la Tabla 36, en la primera ronda se alcanzó el consenso en todos los pasos e indicadores, ya que la desviación estándar no fue mayor que 2.0, por lo que no fue necesaria una segunda ronda. Lo anterior demuestra la claridad en la formulación de la Metodología MePRiSIA y su inclusión del factor humano en todos los pasos.

Sin embargo, los indicadores que estuvieron cerca de no alcanzar el consenso por parte de los expertos fueron:

- **Paso 1: Establecimiento del Contexto**

  Indicador: Fácil de implementar

  Variación Estándar: 1,73

  Explicación: El experto interno señala que las instituciones le han restado por años importancia a la seguridad y la alta dirección no destina recursos a la prevención de riesgos, por lo que se los primeros que deben concientizarse son las personas de la alta dirección para destinen recursos financieros y personal para realizar esta labor. Sin embargo, estos son factores que están fuera del alcance de la metodología

- **Paso 2: Identificación de Riesgos**

  Indicador: Fácil de entender

  Variación Estándar: 1

Explicación: Uno de los expertos externos señala que no es clara la forma en que se deben evaluar los activos de personal. Por dicha razón, se explicó mejor en la metodología en qué consiste dicha evaluación.

Indicador: Fácil de implementar

Variación Estándar: 1

Explicación: El experto interno señala que se debe contar con un grupo de expertos, además de personal de la entidad, para llevar a cabo este paso. Según concepto propio, para identificar los riesgos, se requiere sin duda conocer muy bien los activos y los incidentes que los han afectado, que deberían documentarse adecuadamente cuando ocurran. Además, se debe tener cierto conocimiento en seguridad para identificar las vulnerabilidades.

- **Paso 3: Análisis de Riesgos**

  Indicador: Fácil de implementar

  Variación Estándar: 1

  Explicación: El experto interno señala que para realizar este paso se requiere de expertos en administración de riesgos como de personal experto en las situaciones identificadas. Según concepto propio, son las personas encargadas de los activos las que deben contar con la información suficiente para realizar una valoración adecuada de los riesgos. Además, si es bueno que dentro del personal de TI o el equipo encargado de llevar a cabo la metodología haya al menos un experto en seguridad informática.

- **Paso 4: Prevención de Riesgos**

  Indicador: Fácil de implementar

  Variación Estándar: 1,53

  Explicación: El experto interno señala de nuevo la poca inversión en seguridad y la falta de compromiso de la alta gerencia con este tema. Como se mencionó anteriormente, estos son factores que están fuera del alcance de la metodología

Como se puede apreciar, el indicador más crítico es la implementación de la metodología, pero si una institución decide que su personal de TI o personal externo lleve a cabo la metodología, es claro que debe asignar recursos para que se puedan implementar los controles, porque no tiene sentido hacer un análisis de riesgos para que quede solo en papel y no se tome ninguna acción.

8 CONCLUSIONES

Del estado del arte se puede concluir que:

- El concepto de prevención se aplica en diferentes contextos, como: el democrático, el de la salud, el social, el de la educación y el de las redes computacionales. Aunque las medidas adoptadas para prevenir los daños son diferentes de un contexto a otro, existen características comunes que ayudaron a construir una definición adecuada para los sistemas de información académica, como: "el conjunto de estrategias dirigidas a evitar o reducir los daños causados por los incidentes de seguridad que pueden presentarse en un sistema de información mediante la definición de políticas, la concientización de los usuarios y la mitigación de vulnerabilidades y amenazas".

- La prevención debe constar de un enfoque a largo plazo, en el que se toman medidas de seguridad enfocadas a evitar que ocurran los incidentes como: el establecimiento de políticas, el desarrollo de programas de concientización etc.; y de un enfoque a corto plazo, que busca la reacción rápida ante los incidentes que se estén presentando, a fin de evitar daños mayores, analizando las causas e instaurando las medidas de seguridad necesarias para que no ocurran nuevamente.

- El concepto de riesgo ha evolucionado desde sus inicios en los juegos de azar hasta su incorporación en áreas como la ciencia y la ingeniería, llegando incluso a estandarizarse. Esto llevó a definir el riesgo en los sistemas de información académica como: "la probabilidad de que un evento adverso ocurra y afecte a un sistema de información y a sus activos asociados (personas, información, infraestructura) como resultado de la combinación de una amenaza de seguridad y una vulnerabilidad, causando pérdidas o daños a la organización".

- La valoración del riesgo no consiste solamente en identificar las fallas técnicas sino también en identificar cuestiones sociales como la percepción del riesgo, el sesgo cultural, la falta de concientización y las fallas en la comunicación humana..

- Se debe tener en cuenta que la prevención de riesgos es un proceso continuo, consistente en analizar los riesgos existentes en un sistema, planear y ejecutar actividades, a corto y largo plazo, tendientes a evitar o reducir esos riesgos identificados, evaluar la efectividad de dichas actividades y actualizarlas, de acuerdo a los cambios en el entorno interno y externo de la organización. Por tanto, los sistemas no son entes aislados y estáticos, sino que son influenciados constantemente por su entorno y se van adaptando a él, lo que hace que las medidas de seguridad adoptadas también deban cambiar para ajustarse a los cambios del sistema.

- De las siete metodologías de gestión de riesgos estudiadas, solo tres consideran el factor humano (OCTAVE, MAGERIT y Metodología de Gestión de Riesgos según NIST) y cuatro no lo

consideran de manera explícita (CORAS, Metodología de Administración de Riesgos del Estándar Australiano, NTC-ISO /IEC 27005 y CRAMM). Por su parte, las metodologías de prevención de riesgos estudiadas si consideran el factor humano, principalmente la Metodología para el Diagnóstico, Prevención y Control de la Corrupción en Programas de Seguridad Ciudadana según el BID.

- De las metodologías de gestión de riesgos, la más completa es la Metodología de Gestión de Riesgos según NIST, ya que incluye las fases de: establecimiento del contexto, identificación de riesgos, análisis de riesgos y tratamiento de riesgos, además proporciona tanto las definiciones como las orientaciones prácticas necesarias para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI. Sin embargo, sería bueno complementar el análisis de riesgos que realiza, teniendo en cuenta las responsabilidades individuales, institucionales y sociales, como lo hace la Metodología para el Diagnóstico, Prevención y Control de la Corrupción en Programas de Seguridad Ciudadana según el BID, lo que podría llevar a implementar estrategias de prevención más completas y efectivas. Por otra parte, .la Metodología de Prevención de Incidentes de Malware según NIST, especifica los cuatro elementos principales de la prevención, brindando una buena guía sobre los aspectos a considerar a la hora de implementar estrategias de prevención.

- Algo que se evidenció en todas las metodologías de prevención y gestión de riesgos estudiadas, al explorar sus lineamientos, es la complejidad en la descripción de lo que se debe realizar en cada paso, pues suelen contar con diferentes anexos que buscan aclarar sus pasos, pero que terminan por confundir al lector.

En cuanto al diseño de la metodología se puede concluir:

- Al existir tantas opciones de metodologías de prevención y gestión de riesgos, era necesario que la metodología diseñada tuviera ciertas características que la distinguieran de las demás. Como las personas somos el eslabón más débil en la cadena de la seguridad era indispensable que la metodología considerara el factor humano en cada uno de sus pasos. Además, se trató de crear una metodología sencilla, fácil de entender y de llevar a cabo.

- La metodología diseñada en este trabajo se llama MePRiSIA (Metodología de Prevención de Riesgos para Sistemas de Información Académica) y se compone de cuatro pasos: en el Paso 1: Establecimiento del Contexto, se idenfican los activos importantes para el sistema de información académica, sus requisitos de seguridad y los objetivos que se persiguen con el análisis de riesgos; en el Paso 2: Identificación de Riesgos, se priorizan los activos y se determinan sus vulnerabilidades y amenazas; en el Paso 3: Análisis de Riesgos, se determina el impacto de cada amenaza y su probablidad de ocurrencia para medir el riesgo y priorizarlo; y en el Paso 4: Prevención de Riesgos, se describen diferentes controles aplicables, según el tipo de vulnerabilidad, considerando los cuatro elementos de la prevención: políticas, concientización, mitigación de vulnerabilidades y mitigación de amenazas.

En cuanto a la aplicación de MePRiSIA al Sistema de Información Académica de la Universidad de Pamplona, se puede concluir que:

- Tomó mucho tiempo y esfuerzo llevar a cabo la metodología puesto que no se contaba con la información completa del sistema de información académica, lo que llevó a hacer algunas suposiciones en cuanto a los activos y sus posibles vulnerabilidades y amenazas, por eso se recomienda que esta metodología la lleve a cabo el personal de TI de cada institución, que son los que, en teoría, podrían contar con toda la información necesaria para su desarrollo.

- Según la valoración de los activos realizada, los 5 activos más importantes de ACADEMUSOFT son: la base de datos de información académica con su respectiva interfaz gráfica (ACADEMUSOFT), el servidor de base de datos de información académica y de autenticación, el personal del CIADTI, los administrativos y el centro de datos donde se encuentran los servidores. Como se puede apreciar, dos de estos activos corresponden al factor humano de la institución.

- Se identificaron siete riesgos de nivel muy alto y son los docentes, el personal de CIADTI, los estudiantes y las políticas del sistema de información académica los que ocupan estos lugares, lo que evidencia la importancia de la creación y la difusión de las políticas de seguridad, así como la concientización y capacitación en seguridad de los usuarios.

En cuanto a la validación de la metodología por expertos:

- La metodología fue evaluada por tres expertos: dos expertos externos en seguridad informática y un experto interno en sistemas de información académica, los cuales determinaron si cada uno de los cuatro pasos de la metodología son fáciles de entender, incluyen el factor humano y son fáciles de implementar. Para ello, se elaboró una rúbrica y se utilizó el método Delphi para determinar si llegaban a un consenso.

- Los resultados de las evaluaciones indican que aunque la metodología es fácil de entender e incluye el factor humano, su implementación es difícil cuando la institución no asigna recursos de personal y financieros para llevarla a cabo, ya que falta concientización por parte de las directivas de las instituciones sobre la importancia de la seguridad informática y la prevención de riesgos.

.

9 BIBLIOGRAFÍA

Alberts, C., & Dorofee, A. (2001). *An Introduction to the OCTAVE Method*: Carnegie Mellon University, Software Engineering Institute.

Alexander, A. G. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información: Óptica ISO 27001:2005*. Bogotá: Alfaomega Colombiana S.A.

Álvarez Marañón, G., & Pérez García, P. P. (2004). *Seguridad Informática para Empresas y Particulares*. Madrid: McGraw Hill.

AS/NZS 4360:1999 -Estándar Australiano, Administración de Riesgos. (1999).

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A Framework for Integrated Risk Management in Information Technology. *Management Decision, 37*(5), 437- 444.

Barreau, D. K. (1995). Context as a Factor in Personal Information Management Systems. *Journal of the American Society for Information Science, 46*(5), 327-339.

Boardman, R. P. (2004). *Improving Tool Support for Personal Information Management.* Unpublished Tesis doctoral, Imperial College, Londres.

Boutros-Ghali, B. (1995). *An Agenda for Peace*. New York: United Nations.

Boutros-Ghali, B. (1996). *An Agenda for Democratization*. New York: United Nations.

Brantingham, P. J., & Faust, F. L. (1976). A Conceptual Model of Crime Prevention. *Crime and Delinquency, 22*(3), 284-296.

British_Standards_Institution. (1991). *Quality vocabulary* (No. BS4778 [Part 3 Section 3.2 = IEC 1990 50(191)]). London: BSI.

BS7799-2. (1999). *Information Security Management -Part 2: Specification for Information Security Management Systems*. London: British Standards Institution.

Burnie, D. (2003). *Science*. Retrieved 02/12/2003, from http://encarta.msn.com/text_761557105_1/Science.html

Bustelo Ruesta, C., & Amarilla Iglesias, R. (2001). Gestión del Conocimiento y Gestión de la Información. *Boletín del Instituto Andaluz de Patrimonio Histórico, VIII*.

Byman, D. (2003). Constructing a Democratic Iraq. *International Security, 28*(1), 47-78.

Campos, A. (1999). La Prevención de Desastres como Objeto Educativo. In *Educación y Prevención de Desastres* (pp. 11-84). San José, Costa Rica: Fondo de las Naciones Unidas para la Infancia, UNICEF.

Campos, E., & Pradhan, S. (2007). *The Many Faces of the Corruption: Tracking Vulnerabilities at the Sector Level*. Washington D.C.: World Bank.

Cano, J. J., & Saucedo Mesa, G. (2015). *VII Encuesta Latinoamericana de Seguridad de la Información*: ACIS.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assesment Process* (No. CMU/SEI-2007-TR-12, ESC-TR-2007-012). Bedford: Carnegie Mellon University.

Carnegie_Commission_on_Preventing_Deadly_Conflict. (1997). *Final Report with Executive Summary*. New York: Carnegie Corporation.

Casassus, J. (2000). *Problemas de la Gestión Educativa en América Latina: La Tensión entre los Paradigmas de Tipo A y el Tipo B*. Retrieved 10/02/2010, from http://pasosvagabundos.com/archivos/Lecturas%20de%20trabajo%20para%20educadores/gestion%20educativa/ploblemas%20gestion%20educ%20en%20al.pdf

Central_Oregon_Community_College. (2003). *Social Science Disciplines*. Retrieved 25/11/2003, from http://www.cocc.edu/admit/shells/trans/social_disciplines.htm

CNIL. (2012). *Methodology for Privacy Risk Management*. Paris: Commission Nationale de l´Informatique et des Libertés (CNIL).

Collins, B., & Mansell, R. (2004). *Cyber Trust and Crime Prevention: A Synthesis of the State-of-the-Art Science Reviews*. London: RMCS Cranfield University and London School of Economics and Political Science.

Concha-EastMan, A. (2004). Violencia Urbana en América Latina y el Caribe: Dimensiones, Explicaciones, Acciones. In S. Rotker (Ed.), *Ciudadanías del Miedo* (pp. 39-53.). Caracas: Rutgers.

Deuchar, S. (2003). *Major Organizations Take to Managing Risk*. Retrieved 04/11/2003, from http://ebiz.co.za/news.asp?pklNewsidZ9626&pklIssueIDZ308

Dickson, G. (1995). Principles of Risk Management. *Quaility in Health Care, 4*, 75-79.

Douglas, M., & Wildavsky, A. (1982). *Risk and Culture*. Berkeley, CA: University of California Press.

Ekblom, P. (1996). *Towards a Discipline of Crime Prevention: a Conceptual Framework*: Home Office Research and Statistical Directorate.

Ekblom, P. (2003). *The Conjunction of Criminal Opportunity: A Framework for Crime Reduction*. London: Home Office Crime and Policing Group, Research Development and Statistics Directorate.

Farrington, D. P., & Welsh, B. C. (2007). *Saving Children from a Life of Crime*. Oxford: Oxford University Press.

Franganillo, J. (2009). Gestión de Información Personal: Elementos, Actividades e Integración. *El Profesional de la Información, 18*(4), 399-406.

Frosdick, S. (1997). The Techniques of Risk Analysis are Insufficient in Themselves. *Disaster Prevention and Management, 6*(3), 165-177.

Fung, P., Kwok, L., & Longley, D. (2003). *Electronic Information Security Documentation.* Paper presented at the Australasian Information Security Workshop (AISW2003) -Conferences in Research and Practice in Information Technology, Adelaide (Australia).

García Mejía, M. (2010). *Metodología para el Diagnóstico, Prevención y Control de la Corrupción en Programas de Seguridad Ciudadana* (No. Documento de Debate #IDB-DP-117): Banco Interamericano de Desarrollo (BID).

Gerber, M., & Von Solms, R. (2005). Management of Risk in the Information Age. *Computer & Security, 24*, 16-30.

Gilling, D. (1997). *Crime Prevention Theory, Policy and Politics*. London: UCL.

Glenn, J. K. (2001). Book Review: Three Social Science Disciplines in Central and Eastern Europe. In *Handbook on Economics, Political, Science and Sociology*: Columbia University Website.

Gómez Fernández, F. (2003). *Desarrollo de una Metodología para el Análisis del Riesgo Volcánico en el Marco de un Sistema de Información Geográfica.* Unpublished Tesis Doctoral, Universidad Complutense de Madrid.

Graham, J., & Bennett, T. (1995). *Crime Prevention Strategies in Europe and North America* (Vol. 28). Helsinki-New York: European Institute for Crime Prevention and Control.

Greene, J. C. (2007). *Mixed Methods in Social Inquiry* (Vol. 9). San Francisco: John Wiley & Sons, Inc.

Hampson, F. O. (2002). *Preventive Diplomacy at the United Nations and Beyond* (Fen Osler Hampson and David M. Malone ed.). Boulder Colorado: Lynne Rienner Publishers.

Hayden, C., & Blaya, C. (2001). Violence et Comportements Agressifs Dans les Écoles Anglaises. In E. Debarbieux & C. Blaya (Eds.), *La Violence en Millieu Scolaire-3- Dix Approaches en Europe* (pp. 43-70.). Paris: ESF.

Hernández Sampieri, R., & Mendoza, C. P. (2008). *El Matrimonio Cuantitativo Cualitativo: El Paradigma Mixto.* Paper presented at the 6to Congreso de Investigación en Sexología, Villahermosa, Tabasco, México.

Holland, C. J., & Van Arsdale, P. W. (1989). Aspectos Antropológicos de los Desastres. In *Desastres Consecuencias Psicosociales: La Experiencia Latinoamericana.* Mexico.

Hope, T. (2002). La Riduzione della Criminalità, la Sicurezza Locale e la Nuova Filosofia del Management Pubblico. *AA.VV. Governare la Sicurezza: Attori, Politiche e Istituzioni in Europa, Numero Speciale di Dei Delitti e Delle Pene*, 207-229.

Humphreys, E. J., Moses, R. H., & Plate, A. E. (1998). *Guide to Risk Assessment and Risk Management*. London: British Standards Institution.

ICONTEC. (2009). *NTC-ISO/IEC 27005: Tecnología de la Información. Técnias de Seguridad. Gestión del Riesgo en la Seguridad de la Información*. Bogotá: ICONTEC.

Infoplease.com.*Information Please: On-Line Dictionary*. Retrieved 25/11/2003, from http://www.infoplease.com/ipd/A0549812.html

International_Commission_on_Intervention_and_State_Sovereignty(ICISS). (2001). The Responsability to Protect: Supplementary Volume. In (pp. 29). Otawa: International Development Research Center.

INVESTOPEDIA.*Replacement Cost*. Retrieved 23/06/2015, from http://www.investopedia.com/terms/r/replacementcost.asp

ISO/IEC_TR_13335-1. (1996). *Information Technology - Guidelines for the Management of IT Security - Part 1: Concepts and Models for IT Security* (1st ed.). Switzerland.

Jacobson, R. V. (1996). *CORA: Cost-of-Risk Analysis. Painless Risk Management for Small Systems*: International Security Technology, Inc.

Jones, W. (2007). *Keeping Found Things Found: The Study and Practice of Personal Information Management*. Burlington, MA: Morgan Kaufmann Publishers.

Jung, C., Han, I., & Suh, B. (1999). Risk Analysis for Electronic Commerce Using Case-Based Reasoning. *International Journal of Intelligent Systems in Accounting, Finance and Management, 8*, 61-73.

Kailay, M. P., & Jarratt, P. (1995). RAMeX: A Prototype Expert System for Computer Security Analysis and Management. *Computers and Security, 14*, 449-463.

Khan Pathan, A.-S. (2010). *The State of the Art in Intrusion Prevention and Detection*. Kuala Lumpur: CRC Press.

Kirkwood, A. S. (1994). Why Do We Worry When Scientists Say There Is No Risk? *Disaster Prevention and Management, 3*(2), 15- 22.

Knepper, P. (2007). *Criminology and Social Policy*. London: Sage.

Krauskopf, D. (2006). *Estado del Arte de los Programas de Prevención de la Violencia en Ámbitos Escolares*. Washington: Organización Panamericana de la Salud.

Kroeger, A., & Luna, R. (1992). *Atención Primaria de Salud: Principios y Métodos*. México: COMPILADORES.

Lansdale, M. W. (1988). The Psychology of Personal Information Management. *Applied Ergonomics, 19*(1), 55-66.

Lara Ruiz, Á. (2013). *Algunas Orientaciones para Evaluar los Factores de Riesgo Psicosocial*. Madrid: Instituto Nacional de Seguridad e Higiene en el Trabajo.

Lavrakas, P. J. (1995). Community-Based Crime Prevention: Citizens, Community Organizations and the Police. In L. B. Joseph (Ed.), *Crime, Communities and Public Policy*. Chicago: University of Chicago, Center for Urban Research and Policy Studies.

Lichtenstein, S. (1996). Factors in the Selection of a Risk Assessment Method. *Information Management and Computer Security, 4*(4), 20-25.

Lindblom, L. (2003). *Democracy and the Evolution of a Culture of Prevention: Lessons from Guatemala 1993-2003*: University of Uppsala.

Lizarazo Rueda, J. E. (2012). El Ser Humano: Factor Clave en la Seguridad de la Información. *Apuntes de Investigación, 3*.

Lund, M. S. (2001). From Lessons to Action. In *Reaction to Conflict Prevention* (Fen Osler Hampson and David M. Malone ed., pp. 161). Boulder Colorado: Lynne Rienner Publishers.

Mell, P., Kent, K., & Nusbaum, J. (2005). *Guide to Malware Incident Prevention and Handling*. Gaithersburg: National Institute of Standards and Technology (NIST).

Merino Bada, C., & Cañizares Sales, R. (2011). *Implementación de un Sistema de Gestión de Seguridad de la Información según ISO 27001: Un Enfoque Práctico*. Madrid: FC Editorial.

Miami-Dade_Community_College. (2003). *Social Science Department: Disciplines*. Retrieved 25/11/2003, from http://www.mdcc.edu/kendall/social/disciplines.htm

Ministerio_de_Salud. (1993). *Ley 60 de 1993*.

Moses, R. H. (1992). Risk Analysis and Management. In K. M. Jackson & J. Hruska (Eds.), *Computer Security Reference Book*. Oxford: Butterworth-Heinemann Ltd.

Muñoz Giraldo, G. I. (2004). Historia de la Prevención. *Hacia la Promoción de la Salud, 9*, 27-32.

NIST. (1995). *An Introduction to Computer Security*. Washington: U.S. Department of Commerce.

NIST. (2001). *Risk Management Guide for Information Technology Systems* (Vol. Special publication .). Washington: U.S. Department of Commerce.

Norsk_Regnesentral. (2000). *CORAS: A Platform for Risk Analysis of Security Critical Systems* (No. IST-2000-25031).

Olsen, G. R. (2002). Promoting Democracy, Preventing Conflict: The European Union and Africa. *International Politics, 39*, 311-328.

Original Roget's Thesaurus of English Words and Phrases. (5th ed.)(1992). Essex, England: Longman Group UK Limited.

Owens, S. (1998). *Information Security Management: An Introduction*. London: British Standards Institution.

Oxford Advanced Learner's Dictionary. (5th ed.)(1995). Oxford: Oxford University Press.

Pease, K. (1997). Crime Prevention. In M. Maguire, R. Morgan & R. Reiner (Eds.), *The Oxford Handbook of Criminology* (2 ed., pp. 963-996). Oxford: Oxford University Press.

Peyre, V. (1986). Introduction. Elements d'un Debat Sur la Prévention de la Delinquance. *Annales de Vaucresson, 1*(24), 9-13.

Pfleeger, C. P. (1989). *Security in Computing*. NJ: Prentice Hall.

Pfleeger, C. P. (1997). *Security in Computing* (2nd ed.): Prentice Hall, Inc.

Piper, S. (2011). *Intrusion Detection Systems for Dummies*: WILEY.

Plataforma. (s.f.). *Plataform@ Digital*. Retrieved 01/05/2014, from http://www.unipamplona.edu.co/unipamplona/hermesoft/portalIG/home_28/recursos/gestasoft/28042008/gestasoft_inicio.jsp

PMI. (2008). *A Guide to the Project Management Body of Knowledge (PMBOK Guide)* (4ta ed.). Pennsylvania: Project Management Institute.

Ponjuan Dante, G. (2004). Gestión de Información: Dimensiones e Implementación para el Éxito Organizacional. In *Nuevo Paradigma*. Rosario (Argentina).

Qasem, M. M. d. (2013). Information Technology Risk Assessment Methodologies: Current Status and Future Directions. *International Journal of Scientific & Engineering Research, 4*(12), 966-972.

Ragmognino, N., FradJi, D., Soldini, F., & Vergés, P. (1997). L'École Comme Dispositive Simbolique et les Violences: le Example de Trois Ecoles em Marseille. In B. Charlot & J. C. Émin (Eds.), *Violences à l'école - État des Savoirs.* París: Masson & Armand Colin.

Ramos Lara, K. J. (2014). Sistema de Índices para la Valoración de los Activos Intangibles. *Contribuciones a la Economía*.

Real_Academia_Española.*Eclecticismo*. Retrieved 25/04/2015, from http://lema.rae.es/drae/?val=eclecticismo

Real_Academia_Española.*Pragmatismo*. Retrieved 25/04/2015, from http://lema.rae.es/drae/?val=pragmatismo

Robert, P. (1991). Les Chercheurs Face Aux Politiques de Prévention. In P. Robert (Ed.), *Les Politiques de Prévention de la Delinquance a L'aune de la Recherche. Un Bilan International* (pp. 13-27). Paris: L'Harmattan.

Rosenblum-Kumar, D. Deconstructing Prevention: A Systems Approach to Mitigating Violent Conflict. In *Reaction to Conflict Prevention* (Fen Osler Hampson

David M. Malone ed.): Lynne Rienner Publishers.

Roth, G. (2003). *E-commerce and E-business Have Changed the Profile of Corporate Legal Risk*. Retrieved 04/11/2003, from http://estrategy.co.za/news.asp?pklNewsIDZ12125&pklIssueIDZ346&pklCategoryIDZ141

Royal_Society. (1992). *Risk: Analysis, Perception and Management*. London: The Royal Society.

Sánchez, A. (2004). *La Promoción y Prevención* (Escuela de Salud Pública, Universidad de Costa Rica ed.). San José: Casa Costarricense de Seguro Social, CENDESIS.

Savona, E. U. (2004). Ipotesi Per uno Scenario Della Prevenzione. In R. Selmini (Ed.), *(a cura di) La Sicurezza Urbana,* (pp. 273-284). Bologna: Il Mulino.

Scarff, F., Carty, A., & Charette, R. (1993). *Introduction to the Management of Risk*. Norwich: HMSO.

SecurityArtWork.*Introducción al Análisis de Riesgos - Metodologías (II)*. Retrieved 03/08/2015, from http://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

Sinclair, B. (1999). *Report on State Implementation of the Gun-Free Schools Act: School Year 1997-98*. Rockville, MD: Westat.

SINTEF. (2006). *The CORAS Model-Based Method for Security Risk Analysis*. Oslo: SINTEF.

Stark, H. (2003). *Engineering*. Retrieved 02/12/2003, from http://encarta.msn.com/text_761570676_1/Engineering.html

Stedman, S. J. (1995). Alchemy for a New World Order*. Foreign Affairs,* p. 20.

Strutt, J. (1993). *Risk Assessment and Management: The Engineering Approach*: Centre for Industrial Safety and Reliability, Cranfield University.

Suojanen, T. (2000.). *Technical Communication Research: Dissemination, Reception, Utilization.* Unpublished Licentiate Thesis in Translation Studies: English translation and Interpretation., University of Tampere.

Tapias, E. (2013, 20 de Octubre). Investigan Venta de Notas y Títulos Profesionales en Universidad de Pamplona*. Noticias Uno*.

Tashakkori, A., & Teddlie, C. (2008). Quality of Inferences in Mixed Methods Research: Calling for an Integrative Framework. In M. Max Bergman (Ed.), *Advances in Mixed Methods Research* (pp. 101-119). Londres: SAGE Publications Ltd.

Tchankova, L. (2002). Risk Identification - Basic Stage in Risk Management. *Environmental Management and Health, 13*(3), 290-297.

Tonry, M., & Farrington, D. (1995). Strategic Approach to Crime Prevention. In M. Tonry & D. Farrington (Eds.), *Building a Safer Society. Strategic Approaches to Crime Prevention, Crime and Justice* (Vol. 19, pp. 1-20).

U.S._Department_of_Labor. (2003). *Occupational Handbook*: Bureau of Labor Statistics.

U.S._Department_of_State.*Democracy*. Retrieved 03/09/2003, from http://www.state.gov/g/drl/democ/

University_of_Maryland. (2003). *Social Science: Supplemental Major Courses.* Retrieved 25/11/2003, from http://www.umuc.edu/prog/ugp/majors/socs.shtml

Villalba. (2002). *Magerit version 1.0: Risk Analysis and Management Methodology for Information Systems (Procedures Handbook)*.

Walgrave, L., & De Cauter, F. (1986). Une Tentative de Clarification de la Notion de Prévention. *Annales de Vaucresson, 1*(24), 31-51.

Wallensteen, P. (1998). *Preventing Violent Conflicts, Past Record and Future Challenges*: Department of Peace and Conflict Research, Uppsala University.

Wallensteen, P. (2002a). *Reassessing Recent Conflicts: Direct vs. Structural Prevention* (Fen Osler Hampson and David M. Malone ed.). Boulder Colorado: Lynne Rienner Publishers.

Wallensteen, P. (2002b). Understanding Conflict Resolution. In (pp. 271). London: Sage.

Weems, B. S. (2003). *Computer Science*. Retrieved 02/12/2003, from http://encarta.msn.com/text_761563863_1/Computer_Science.htm

Wikipedia.*Reduccionismo*. Retrieved 25/04/2015, from http://es.wikipedia.org/wiki/Reduccionismo

Wilches-Chaux, G. (1998). *Auge, Caída y Levantada de Felipe Pinillo, Mecánico y Soldador o Yo Voy a Correr el Riesgo*. Quito: La Red.

Wordreference.com.*Pragmatismo*. Retrieved 25/04/2015, from http://www.wordreference.com/definicion/pragmatismo

Yu, E. (2004). Information Systems (In the Internet Age). In *Practical Handbook of Internet Computing*: CRC Press.

ANEXOS

A. ARTÍCULO REVISTA SISTEMAS & TELEMÁTICA

Acevedo N. & Satizábal C. (2016). Risk management and prevention methodologies: a comparison. *Sistemas & Telemática*, *14*(36), 39-58.

Discussion paper / Artículo de reflexión - Tipo 2

Risk management and prevention methodologies: a comparison

Nancy Acevedo, Esp. / acevedoquintana@gmail.com

Cristina Satizábal, Ph.D. / cristina.satizabal@unipamplona.edu.co

Universidad de Pamplona, Colombia

ABSTRACT In this paper we analyze nine risk management and prevention methodologies, carrying out a comparison of the stages that they include and determining if they take into account the human factor in the risk analysis and treatment. We observe that only 42.85% of the studied management risk methodologies include this factor and conclude that the NIST [National Institute of Standards and Technology] Risk Management methodology is the most complete, although it would be desirable for it to focus more on the human factor like the IDB [Inter-American Development Bank] Corruption Diagnosis, Prevention and Control in Programs of Civic Security methodology.

KEYWORDS Analysis; management; methodologies; prevention; risks.

Metodologías de gestión y prevención de riesgos: una comparación

RESUMEN En este artículo se analizan nueve metodologías de gestión y prevención de riesgos a través de la comparación de sus fases y de la revisión de si consideran o no al factor humano en el análisis y tratamiento de los riesgos (se observa que menos de la mitad de ellas, esto es 42,85% considera este factor). Las investigadoras concluyen que la metodología de gestión de riesgos del Instituto Nacional de Estándares y Tecnología es la más completa, aunque sería conveniente que se enfocara más en el factor humano, como lo hace la metodología para el diagnóstico, prevención y control de la corrupción en programas de seguridad ciudadana del Banco Interamericano de Desarrollo.

PALABRAS CLAVE Análisis; gestión; metodologías; prevención; riesgos.

Metodologias de gestão e prevenção de riscos: uma comparação

RESUMO Este artigo analisa nove metodologias de gestão e prevenção de riscos, comparando as suas fases e analisa-se se devem ou não considerar o fator humano na análise e tratamento de riscos (observa-se que menos de metade delas, isto é 42,85% consideram esse fator). As investigadoras concluem que a metodologia de gestão de riscos do Instituto Nacional de Estándares e Tecnologia é a mais completa, embora fosse conveniente se focar mais no factor humano, como o faz a metodologia para o diagnóstico, prevenção e controle da corrupção em programas de segurança cidadã do Banco Interamericano de Desenvolvimento.

PALAVRAS-CHAVE Análise; gestão; metodologias; prevenção; riscos.

This paper is an output from the research project: Methodology for risk prevention on the management of personal information filed in the academic information system of Universidad de Pamplona / Este artículo es producto del proyecto de investigación: Metodología para la prevención de riesgos en el manejo de la información personal almacenada en el sistema de información académica de la Universidad de Pamplona. (Convocatoria de Banco de Proyectos 2014 - Vicerrectoría de Investigaciones, Universidad de Pamplona. Código: PR130-00-21 (GA190-CM-I-2014-2.1.2.2.1).

Received / Recepción: Enero 7, 2016 - Accepted / Aceptación: Marzo 1, 2016

doi: 10.18046/syt.v14i36.2214

I. Introduction

Effective use of information and communications technologies [ICT] is a critical factor of success in current society. Most failures are not caused by the technology itself, but rather by the manner in which it is used (Yu, 2004). Due to the misuse of personal information, many users have been victims of fraud and extortion through the Internet, yet most such incidents could be prevented if the risks were properly analyzed, and the appropriate prevention strategies for each context were implemented.

Although engineering focuses more on technology than on people (Frosdick, 1997), engineers know that "risk perception depends largely on beliefs, feelings and judgments, and has great influence on tolerance or acceptance of risk" (Strutt, 1993). However, the techniques used in engineering are more concerned with identifying technical failures than social matters such as risk perception, cultural bias, and failures in human communication.

Social scientists are strongly opposed to the vision of natural scientists and engineers regarding risk management, and warn that ignoring sociological or social questions can be problematic, since the result of a human error –or of the lack of communication– can be as disastrous as the result of a technical failure (Frosdick, 1997).

So, it is crucial to conduct a review of the methodologies of the management and prevention of existing risks, to identify common and distinctive characteristics of each, and to determine whether the human factor is considered.

In section II, prevention and risk concepts from different contexts are defined; section III describes the different management methodologies and risk prevention found in the literature; in section IV, aspects for comparing the different methodologies are identified; in section V different methodologies are compared; and section VI presents the conclusions.

II. Definitions

Risk

A timeline showing how the concept of risk has evolved in different contexts is presented in Table 1.

Prevention

At a democratic level, the concept of conflict prevention is used, having gained attention after the Cold War due to the awareness of the dangers of intra-state war and the collapse of states used (Weiss & Hubert, 2001).

Conflict prevention strategies can be divided into two categories: structural prevention, and direct or operational prevention

I. Introducción

El uso eficiente de las Tecnologías de la Información y las Comunicaciones [TIC] se ha convertido en un factor de éxito crítico para la sociedad actual. La mayoría de las fallas no se deben a la tecnología en sí, sino a la manera en que ella se usa (Yu, 2004). Debido al uso inadecuado de la información personal, muchos usuarios han sido víctimas de fraude y extorsión a través de Internet, sin embargo, la mayoría de estos incidentes se podría evitar si se analizan adecuadamente los riesgos y se implantan estrategias de prevención adecuadas a cada contexto.

Aunque la ingeniería se centra más en la tecnología que en las personas (Frosdick, 1997), los ingenieros saben que "la percepción del riesgo depende en gran medida de las creencias, sentimientos y juicios, y tiene gran influencia sobre la tolerancia o aceptación del riesgo" (Strutt, 1993). Sin embargo, las técnicas utilizadas en la ingeniería se preocupan más por la identificación de las fallas técnicas, que por cuestiones sociales como: la percepción del riesgo, el sesgo cultural y las fallas en la comunicación humana.

Los científicos sociales se oponen fuertemente a la visión de los científicos naturales y de los ingenieros en cuanto a la gestión de riesgos y advierten que hacer caso omiso de las cuestiones sociológicas o sociales podría resultar problemático, ya que el resultado de un error humano –o de la falta de comunicación– puede ser tan desastroso como el resultado de una falla técnica (Frosdick, 1997).

Por lo dicho, es de vital importancia hacer una revisión de las metodologías de gestión y prevención de riesgos existentes, identificar las características comunes y distintivas de cada una de ellas, y determinar si consideran el factor humano.

En la sección II se definen los conceptos de prevención y riesgo desde diferentes contextos, en la sección III se describen las diferentes metodologías de gestión y prevención de riesgos encontradas en la literatura, en la sección IV se identifican los aspectos a comparar en las diferentes metodologías, en la sección V se comparan las diferentes metodologías y en la sección VI se presentan las conclusiones.

II. Definiciones

Riesgo

En la Tabla 1 se presenta una línea de tiempo que permite apreciar cómo ha evolucionado el concepto de riesgo en los diferentes contextos.

Prevención

A nivel democrático se utiliza el concepto de prevención de conflictos, que ganó gran atención después de la Guerra Fría, debido a la concientización que hubo sobre los peligros que acarrea la guerra intra-estatal y el colapso de los Estados (Weiss & Hubert, 2001).

Date	Hito	Benchmark
Siglo XVII	Matemáticas de juegos de azar: "El riesgo es una comparación entre la probabilidad y la magnitud de las pérdidas y las ganancias potenciales". (Douglas,1990)	Mathematics associated with gambling:"Risk referred to a combination between probability and magnitude of potential gains and losses". (Douglas,1990)
Siglo XVIII	Negocios de los seguros marítimos: Riesgo todavía considerado como las ganancias y las pérdidas. (Douglas,1990)	Marine insurance business: Risk, is still considered both gains and losses. (Douglas,1990)
Siglo XIX	Economía: Riesgo concepto negativo, por lo que se crearon incentivos especiales para que se tomara el riesgo que implicaba la inversión. (Douglas,1990)	Economy: The concept of risk, seen more negatively, caused entrepreneurs to call for special incentives to take the risk involved in investment. (Douglas,1990)
Siglo XX	Ingeniería y Ciencia: "El riesgo es los peligros que plantean los avances tecnológicos modernos en la industria nuclear y petroquímica". (Gerber & Von Solms, 2005)	Engineering and Science: "The risk is the hazards posed by modern technological developments such as in the petro-chemical and nuclear industries"(Gerber & Von Solms, 2005)
1991	Estándar Británico 4778: "El riesgo es la combinación de la probabilidad o de la frecuencia de ocurrencia de un peligro definido y la magnitud de las consecuencias de su ocurrencia". (British Standards Institution,1991)	British Standard 4778: "Risk is 'the combination of the probability or frequency of occurrence of a defined hazard and the magnitude of the consequences of the occurrence". (British Standards Institution, 1991)
1992	Royal Society: "El riesgo es la probabilidad de que un evento adverso particular ocurra durante un periodo de tiempo establecido o resulte de un desafío particular". (Royal Society, 1992)	Royal Society: "The risk is he probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge". (Royal Society, 1992)
1993	Ingenieros saben que "Percepción del riesgo depende en gran medida de las creencias sentimientos y juicios, y tiene gran influencia sobre la tolerancia o aceptación del riesgo". (Strutt, 1993).	Engineers know that "Risk perception depends very much on beliefs, feelings and judgements [and] has major influence on the tolerability or acceptance of risk". (Strutt, 1993).
	Paradigma de las Ciencias Naturales: "Riesgo objetivo o evaluado, debido a los métodos científicos de la valoración.	Paradigm of Natural Sciences: "Target risk or evaluated, because scientific methods of valuation.
	Evaluación objetiva del riesgo sigue cálculos precisos, formulas y experimentos exactos".(Kirkwood,1994)	Objective risk assessment remains accurate calculations formulas and exact experiments". (Kirkwood, 1994)
1994	Paradigma de las Ciencias Sociales: "Riesgo subjetivo o percibido, decisión a la que se llegó sin una evaluación científica. Evaluación subjetiva del riesgo se basa en percepción, heurística o decisión a la que se llega mediante la utilización de experiencia, juicio e ingenio" (Kirkwood,1994)	Paradigm of Social Sciences: "Subjective or perceived risk, since it is a decision, which is arrived at without a scientific assessment. The subjective risk evaluation is based on perception, heuristics or rule-of-thumb guidelines. Rule-of-thumb being a decision arrived at by utilizing experience, judgment and ingenuity" (Kirkwood,1994)
1995	Ambiente Computacional: "El riesgo es el potencial del daño aun sistema, o a los activos asociados, que existe como resultado de la combinación de una amenaza de seguridad y una vulnerabilidad". (Kailay & Jarratt, 1995)	Computational Environment: "The risk is the potential for damage to a system or associated assets that exists as the result of a combination of a security threat and vulnerability. The risk exists because of the combination of threats, vulnerability and asset value". (Kailay & Jarratt, 1995)
	NIST: "El riesgo es la posibilidad de que ocurra algo adverso" (NIST,1995)	NIST: "The risk as the possibility of something adverse happening". (NIST,1995)
1996	ISO/IEC TR 13335-1 "El riesgo comprende una combinación de activos, amenazas y vulnerabilidades". (ISO/IEC TR 13335 1, 1996)	ISO / IEC TR 13335-1 "Risk comprises a combination of asset, threat and vulnerability". (ISO/IEC TR 13335 1, 1996)
1997	Frosdick: El análisis de los riesgos es la suma de identificación, estimación y evaluación del riesgo. (Frosdick, 1997)	Frosdick: The risk analysis is the sum of risk identification, estimation and evaluation. (Frosdick, 1997)
1999	La gestión de riesgos debe ir precedida de una actividad de análisis de riesgos. (Bandyopadhyay, Mykytyn & Mykytyn, 1999; Owens, 1998; BS 7799-2, 1999; Moses, 1992)	Risk management should be preceded by some risk analysis activity. (Bandyopadhyay, Mykytyn & Mykytyn, 1999; Owens, 1998; BS 7799-2, 1999; Moses, 1992)
2001	NIST: "El riesgo es el impacto negativo neto debido a una vulnerabilidad considerando su probabilidad y el impacto de ocurrencia". (NIST, 2001)	NIST : "The risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence". (NIST, 2001)
	Australian/ New Zealand Standard: "La gestión del riesgo es un proceso iterativo conformado por pasos bien definidos que llevados a cabo de manera secuencial, constituye el fundamento para la adecuada toma de decisiones, al proporcionar un mejor conocimiento de los riesgos y del impacto de los mismos". (Martínez López, 2001)	Australian/New Zealand Standard: "Risk management is an iterative process consisting of well-defined steps carried out sequentially, it is the basis for proper decision making by providing a better understanding of the risks and the impact of them". (Martínez López, 2001)

Table 1. Evolution of the risk concept / Evolución del concepto de riesgo

(Wallensteen, 2002). Structural prevention incorporates measures to ensure that a crisis does not arise in the first place, and if it does, to avoid repetition. Operational or direct prevention consists of measures to address an immediate crisis (Carnegie Corp., 1957). The choice between structural or direct prevention depends on the areas of disagreement, the appropriate time to implement the preventive action, the levels at which preventive measures should be applied, and the different theories on the causes of conflict and how these should be treated (Wallensteen & Möller, 2003).

In the health field, the concept of prevention is related to the health–disease process (disease prevention). In every period of history there have been different interpretations of health and disease, which are in turn related to the political, economic and social situations of each historical moment (García-Ospina & Tobón-Correa, 2000).

Prevention was described by Henry Sigerist (1951) as one of the three functions of medicine, along with repair or treatment of injury and rehabilitation. Later, Americans classified it as a function of public health.

Prevention has been defined by the World Health Organization as "the application of technical measures including medical aspects and other disciplines that aim to prevent the onset of disease –primary prevention–, heal –secondary prevention–, and restore lost abilities –tertiary prevention" (OMS, 1986 cited by Sánchez-Peña, Sánchez-Delgado, & Agudelo-Ramírez, 2015).

Prevention in the social context is identified at a glance at first look a set of actions that can eliminate or reduce conditions of criminality present in society, when warning signs have not yet been shown, and may include measures aimed at groups at criminal risk or a criminal event that has already been committed, to prevent a subsequent recurrence (Brantingham & Faust, 1976).

In an analysis of prevention programs performed in Belgium during the 1980s, Walgrave and De Cauter (1986) critically analyzed a classification based on the distinction between the moments at which the preventive action is involved –before, during or after the unwanted event–, the focus of preventive intervention –the behaviors of subjects or modification of the social context–, and the defensive orientation –about symptoms– or offensive orientation –about the causes. Thus, social prevention is not a specific action or one of the numerous modalities of prevention, but rather a global policy, oriented to the social welfare, that cuts across all sectors of administrative policy (Graham & Bennett, 1995; Knepper, 2007; Peyre, 1986; Walgrave & De Cauter, 1986).

Las estrategias de prevención de conflictos se pueden dividir en dos categorías: prevención estructural y prevención directa u operacional (Wallensteen, 2002). La prevención estructural incorpora medidas para asegurar que la crisis no surja, en primer lugar, y si lo hace, que no se repita. La prevención operacional o directa consta de medidas para enfrentar crisis inmediatas (Carnegie Corp., 1957). La elección entre prevención estructural o directa depende de las áreas de desacuerdo, el tiempo apropiado para implantar la acción de prevención, los niveles en que las medidas preventivas deben ser aplicadas, así como de las diferentes teorías sobre las causas de los conflictos y de cómo estos deben ser tratados (Wallensteen & Möller, 2003).

En el campo de la salud, el concepto de prevención está ligado al proceso salud-enfermedad (prevención de enfermedades). En cada época de la historia se han dado diferentes interpretaciones a la salud y a la enfermedad, las cuales, a su vez, se relacionan con las situaciones políticas, económicas y sociales de cada momento histórico (García-Ospina & Tobón-Correa, 2000).

La prevención fue descrita por Henry Sigerist (1951) como una de las tres funciones de la medicina, junto con la reparación o el tratamiento del daño y la rehabilitación. Más adelante, los norteamericanos las denominaron como funciones de la salud pública.

La prevención ha sido definida por la Organización Mundial de la Salud como: "la aplicación de medidas técnicas que incluyen aspectos médicos y de otras disciplinas que tienen como finalidad impedir la aparición de la enfermedad –prevención primaria–, curarla –prevención secundaria– y devolverle las capacidades perdidas –prevención terciaria–" (OMS, 1986 citada por Sánchez-Peña, Sánchez-Delgado, y Agudelo-Ramírez, 2015).

La prevención en el contexto social se identifica a simple vista como el conjunto de acciones que permite eliminar o reducir las condiciones de criminalidad presentes en lo social, cuando todavía no se han manifestado señales de peligro, y puede comprender medidas dirigidas a grupos en riesgo delictivo o a un evento criminal que ya ha sido cometido, para prevenir posteriores recaídas (Brantingham & Faust, 1976).

En un análisis de los programas preventivos realizado en Bélgica durante los años 80, Welgrave y De Cauter (1986) analizaron críticamente una clasificación basada en la distinción entre los momentos en los que interviene la acción preventiva –antes, durante o después del evento indeseado–, el enfoque de la intervención preventiva –los comportamientos de los sujetos o la modificación del contexto social– y la orientación defensiva –sobre los síntomas– u ofensiva –sobre las causas–. Entonces, la prevención social no es una acción específica o una de las numerosas modalidades de prevención, sino una política global orientada al bienestar social que atraviesa todos los sectores de las políticas administrativas (Graham & Bennett, 1995; Knepper, 2007; Peyre, 1986; Walgrave & De Cauter, 1986).

Tonry y Farrington (1995) rechazan esta visión amplia y, con la intención de ser más claros, separan la prevención social en dos partes: una, relativa a las motivaciones individuales, la otra, al contexto social. La prevención social es simple: considerando que los comportamientos criminales son el resultado de predisposiciones y oportunidades, se intenta modificar las predisposiciones, cuanto sea posible, pasando después a modificar las oportunidades (Savona, 2004).

En el campo de la educación, la prevención de la violencia en la escuela se compone de dos vertientes: la de la salud pública y la de los derechos. En el campo de la salud pública: la prevención primaria busca fomentar un ambiente social e individual de respeto y tolerancia, de valores sociales y de conducta personal que favorezca que los conflictos se resuelvan de maneras no violentas, o sea, se dirigen a evitar que ocurra el hecho violento (Concha-EastMan, 2004); la prevención secundaria busca detener precozmente o retardar el progreso de la violencia o de sus secuelas en cualquier punto de su aparición (Vargas, Villegas, Sánchez, & Holthuis, 2003), se aplica cuando un evento violento ya ha ocurrido, y su intención es evitar nuevos episodios o disminuir su gravedad (Concha-EastMan, 2004); y la prevención terciaria se orienta a reducir las complicaciones y consecuencias de los daños de la violencia, en ella adquiere importancia la rehabilitación para mejorar la calidad de vida (Vargas et al., 2004).

Existen variables internas –endógenas– y externas –exógenas– que intervienen en la prevención de la violencia escolar. Las variables endógenas se refieren a factores que podríamos llamar instrumentales o directos, como los sistemas de normas y reglamentos, así como los proyectos político-pedagógicos (Hayden & Blaya, 2001; Ragmognino, Fradji, Soldini, & Vergès, 1997). Las variables exógenas, por su parte, están relacionadas con las habilidades vinculadas a aprender, a ser y a convivir, que cubren una amplia gama de capacidades, tales como: asumir retos en lo académico; establecer relaciones humanas estables y satisfactorias; mantener la esperanza sobre el futuro; y tomar decisiones oportunas, adecuadas, efectivas y constructivas.

La prevención en el contexto educativo debe fortalecer cuatro capacidades fundamentales: permitir al alumno establecer vínculos de calidad en diversos contextos; ser eficaz en situaciones de estudio-trabajo, movilizando la energía y el esfuerzo precisos para ello, y obteniendo el reconocimiento social necesario; integrarse en grupos de iguales constructivos, resistiendo presiones inadecuadas; y desarrollar una identidad propia y diferenciada que le ayude a encontrar su lugar en el mundo y le permita apropiarse de su futuro (Díaz-Aguado, Martínez-Arias, & Martín-Seoane, 2004).

La prevención, en el contexto de las redes computacionales, significa mantener a los atacantes alejados –es decir, prevenir que los atacantes entren a la red– (Khan-Pathan, 2010), es así como se habla de la prevención de crímenes

Tonry and Farrington (1995) reject this wide vision and intend to be clearer, stating that social prevention is separated into two parts: one related to individual motivations, the other to the social context. Social prevention is simple: considering that criminal behavior is the result of predispositions and opportunities, the intention is to change the predispositions as far as possible, then to modify the opportunities (Savona, 2004).

In the field of education, the prevention of violence at school consists of two aspects: public health and rights. In the field of public health, primary prevention seeks to promote a social and individual environment of respect and tolerance, social values and personal behavior that favors a resolution of non-violent conflict, i.e., the goal is to prevent the violent event occurring (Concha-Eastman, 2004); secondary prevention aims to stop promptly or slow the progress of violence or its sequel at any point that it appears (Vargas, Villegas, Sanchez, & Holthuis, 2003). This applies when a violent event has already occurred, and their intention is avoid new episodes or reduce their severity (Concha-Eastman, 2004). Tertiary prevention aims to reduce the complications and consequences of the harm of violence, and it is here that rehabilitation becomes important to improve the quality of life (Vargas et al., 2004).

There are internal –endogenous– and external –exogenous– variables involved in preventing school violence. The endogenous variables relate to factors that might be called instrumental or direct, such as systems of rules and regulations, as well as political–pedagogical projects (Hayden & Blaya, 2001; Ragmognino, Fradji, Soldini, & Vergès, 1997). The exogenous variables, meanwhile, are related to learning skills; to be, and to coexist; covering a wide range of capabilities, such as taking on academic challenges; establishing stable and favorable human relations; maintaining hope for the future; and taking timely, appropriate, effective and constructive decisions.

Prevention in the educational context should strengthen four fundamental capabilities: enabling students to establish quality links in different contexts; being effective in work–study situations, mobilizing the energy and precise effort to do so, and obtaining the necessary social recognition; integrating groups of equal construction, resisting pressures adequately; and developing a distinct identity that helps you find your place in the world and enables you to appropriate its future (Díaz-Aguado, Martínez-Arias, & Martín-Seoane, 2004).

Prevention in the context of computer networks means keeping attackers at a distance –that is, preventing attackers from entering the network– (Khan-Pathan, 2010), and thus it speaks of cybercrime prevention, incident prevention and intrusion prevention.

Crime prevention in the context of cyberspace means reducing the risk of the occurrence of the crime and the potential gravity of the crime, and disorderly events that may occur, both on-line and off-line (Ekblom, 2003).

In the prevention of accidents, on the other hand, there are four main elements: policies, which are the basis for implementing preventive controls; awareness to reduce the number of incidents that occur by human error; mitigating vulnerabilities to eliminate some possible attack vectors; and mitigation of threats to prevent attacks on different systems and networks from being successful (Mell, Kent, & Nusbaum, 2005).

An intrusion prevention system [IPS] is a device or program used to detect signs of intrusion in networks or systems and to take action. Such action consists in generating alarms or blocking intrusions in an active way (Piper, 2011).

III. Risk management and prevention methodologies

Octave

Octave is a risk analysis methodology developed by Carnegie Mellon University in 2001. Its name is an acronym for Operationally Critical Threat, Asset and Vulnerability Evaluation. Octave studies the risks based on three principles: confidentiality, integrity and availability. This methodology is used by different government agencies such as the United States Department of Defense [DoD] (Huerta, 2012). The three phases of this methodology are defined as follows (Alberts & Dorofee, 2001):

- Phase 1: Build profiles based on active threats: important information assets, threats to assets, security requirements of the assets, the actions that the organization is taking to protect them, and weaknesses in organizational policies and practices are identified.
- Phase 2: Identify infrastructure vulnerabilities: key operating components of information technologies are examined for technological vulnerabilities that could lead to an unauthorized action.
- Phase 3: Develop strategies and security plans: the information generated in Phases 1 and 2 is analyzed to identify business risks and assess risks based on their impact on the mission of the organization. In addition, a protection strategy is developed, for organizational plans and mitigation which address the risks of highest priority.

CORAS

CORAS is a European research and technological development project. In the CORAS method an analysis of security risks is carried out in seven steps (Boge, 2001):

cibernéticos, prevención de incidentes y prevención de intrusos.

La prevención del crimen, en el contexto del ciberespacio, significa reducir el riesgo de ocurrencia del crimen y la gravedad potencial del crimen y de eventos desordenados que pueden ocurrir, tanto en línea, como fuera de línea (Ekblom, 2003).

En la prevención de incidentes, por otra parte, existen cuatro elementos principales: políticas, que son la base para implementar controles preventivos; concientización, para reducir el número de incidentes que ocurren por errores humanos; mitigación de vulnerabilidades, para eliminar algunos posibles vectores de ataque; y mitigación de amenazas, para prevenir que las amenazas de diferentes sistemas y redes atacantes sean exitosas (Mell, Kent, & Nusbaum, 2005).

Un sistema de prevención de intrusos [*Intrusion Prevention System, IPS*] es un dispositivo o programa utilizado para detectar señales de intrusión en las redes o sistemas y tomar una acción. Dicha acción consiste en generar alarmas y/o bloquear las intrusiones de manera activa (Piper, 2011).

III. Metodologías de gestión y prevención de riesgos

Octave

Octave es una metodología de análisis de riesgos desarrollada por la Universidad Carnegie Mellon en 2001, su acrónimo significa *Operationally Critical Threat, Asset and Vulnerability Evaluation*. Octave estudia los riesgos con base en tres principios: confidencialidad, integridad y disponibilidad. Esta metodología es utilizada por distintas agencias gubernamentales, tales como el Departamento de Defensa de Estados Unidos [DoD] (Huerta, 2012). Las tres fases de esta metodología se definen así (Alberts & Dorofee, 2001):

- Fase 1: construir perfiles de amenazas basados en activos: se identifican los activos de información importantes, las amenazas a los activos, los requisitos de seguridad de los activos, lo que la organización está haciendo para protegerlos y las debilidades en las políticas y prácticas organizacionales.
- Fase 2: identificar vulnerabilidades de la infraestructura: los componentes operativos clave de las tecnologías de información se examinan en busca vulnerabilidades tecnológicas que puedan conducir a una acción no autorizada.
- Fase 3: desarrollar las estrategias y los planes de seguridad: la información generada en las fases 1 y 2 se analiza para identificar riesgos para la empresa y evaluar los riesgos en función de su impacto en la misión de la organización. Además, se desarrolla una estrategia de protección para los planes de la organización y de mitigación que aborde los riesgos de más alta prioridad.

CORAS

Coras es un proyecto de investigación y desarrollo tecnológico europeo. En el método CORAS un análisis de riesgos de seguridad se lleva a cabo en siete pasos, así (Boge, 2001):

- Paso 1: reunión introductoria donde los representantes del cliente presentan sus objetivos generales de análisis y lo que desean analizar.
- Paso 2: reunión con los representantes del cliente, donde los analistas presentan su comprensión de lo que entendieron en la primera reunión y el estudio de la documentación que puso a su disposición el cliente; este segundo paso implica también un análisis básico de la seguridad de alto nivel.
- Paso 3: descripción más precisa del objeto a analizar y de todos los supuestos y otras condiciones previas hechas. Este paso termina cuando toda esta documentación ha sido aprobada por el cliente.
- Paso 4: taller con personas con experiencia en el objeto del análisis, realizado con el objetivo de identificar el mayor número de posibles incidentes no deseados como sea posible, así como las amenazas, vulnerabilidades y escenarios de amenaza.
- Paso 5: taller enfocado en la estimación de las consecuencias y de los valores de probabilidad para cada uno de los incidentes no deseados identificados.
- Paso 6: entrega al cliente del primer cuadro de riesgo general, lo que normalmente da lugar a algunos ajustes y correcciones.
- Paso 7: identificación del tratamiento y abordaje de cuestiones de costo/beneficio de los tratamientos.

Estándar australiano

La metodología de administración de riesgos según estándar australiano se desarrolla en cinco fases, las cuales, de acuerdo con el AS/NZS 4360:1999, son:

- Establecer el contexto: se definen los parámetros básicos de los procesos que ocurren dentro de la estructura organizacional de acuerdo con el contexto estratégico, organizacional y de administración de riesgos, lo que da como resultado el desarrollo de criterios de evaluación y una guía para la toma de decisiones.
- Identificar riesgos: se identifican todos los riesgos a administrar, estén o no bajo control de la organización.
- Analizar riesgos: se separan los riesgos menores de los riesgos mayores y así se proveen datos para su evaluación y tratamiento; esta fase involucra prestar atención a las fuentes de riesgos, sus consecuencias y las probabilidades de que puedan ocurrir esas consecuencias.
- Evaluar riesgos: se compara el nivel de riesgo detectado durante el proceso de análisis con los criterios de riesgo establecidos previamente, el resultado de una evaluación de riesgos es una lista de riesgos con prioridades para una acción posterior, basadas en los objetivos de

- Step 1: Introductory meeting where customer representatives present the overall objectives of their analysis and what they want to analyze.
- Step 2: Meeting with customer representatives, where analysts present their understanding of the concerns put forward at the first meeting and the study of the documentation made available by the client; This second step also involves a basic analysis of high-level security.
- Step 3: Accurate description of the object to be analyzed and of all other preconditions and assumptions made. This step ends when all this documentation has been approved by the customer.
- Step 4: Workshop with people of experience in the subject of the analysis, carried out in order to identify the largest possible number of unwanted incidents, as well as threats, vulnerabilities and threat scenarios.
- Step 5: Workshop focusing on the estimation of the consequences and probability values for each unwanted incident identified earlier.
- Step 6: Customer delivery of the first picture of overall risk, which usually results in some adjustments and corrections.
- Step 7: Identification of treatment and addressing issues of cost/benefit of treatment.

Australian standard

The risk management methodology according to the Australian Standard is divided into five phases, which, according to the AS/NZS 4360: 1999, are:

- Establish the context: The basic parameters of the processes occurring within the organizational structure are defined, according to the strategic, organizational and risk management context, which results in the development of assessment criteria and a guide for decision.
- Identify risks: All risks to be managed are identified, whether or not they are under the control of the organization.
- Analyze risks: Minor risks are separated from major risks and thus data for their evaluation and treatment are provided; this phase involves paying attention to the sources of risks, their consequences and the probabilities that those consequences may occur.
- Evaluate risks: The risk level identified during the analysis process is compared with risk criteria previously established; the result of a risk assessment is a list of

risks prioritized for further action, based on the objectives of the organization and the degree of opportunity there could be to take the risk.

- Address risks: The range of options to address risks is identified, these options are evaluated, and risk treatment plans are prepared and implemented.

NTC-ISO/IEC 27005

This, the technical standard of risk management in information security, includes the following steps in the risk management process:

- Establish the context: This implies establishing the basic criteria necessary for risk management, defining the scope and boundaries, and establishing an appropriate organization for risk management.
- Assessing the risk: This consists in identifying the risks, describing them quantitatively or qualitatively and prioritizing them against the risk evaluation criteria and relevant objectives for the organization. It consists of the identification, estimation, and assessment of the risk.
- Risk identification: Its purpose is to determine what might happen to cause a potential loss, and to understand how, where and why this loss could occur. For this it is necessary to identify: assets, threats, existing controls, vulnerabilities, and consequences.
  - Risk estimation: An estimation methodology may be qualitative or quantitative, or a combination of these, depending on the circumstances; in practice, often qualitative estimation is used first to obtain a general indication of the level of risk and reveal the most significant risks, and subsequently, if necessary, a quantitative analysis of the significant risks is performed, since it is generally less complex and less expensive to perform a qualitative analysis than a quantitative one.
  - Risk assessment: Consists in comparing risk levels against criteria for risk assessment and their acceptance criteria.
  - Risk treatment: Consists of selecting controls to reduce, retain, avoid, or transfer risks; a plan for risk treatment should be defined.
- Acceptance of risk: This involves taking the decision to accept the risks and responsibilities for the decision and registering them in a formal way.

1. *Central Communication and Telecommunication Agency*

la organización y el grado de oportunidad que podría resultar al tomar el riesgo.

- Tratar los riesgos: se identifica el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos.

NTC-ISO/IEC 27005

Esta, la norma técnica de gestión del riesgo en la seguridad de la información, incluye estos pasos en el proceso de gestión del riesgo:

- Establecer el contexto: implica establecer los criterios básicos necesarios para la gestión del riesgo, definir el alcance y los límites, y establecer una organización adecuada para la gestión del riesgo.
- Valorar el riesgo: consiste en identificar los riesgos, describirlos cuantitativa o cualitativamente y priorizarlos frente a los criterios de evaluación del riesgo y los objetivos relevantes para la organización. Se compone de la identificación, estimación y evaluación del riesgo.
  - Identificación del riesgo: su propósito es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender cómo, dónde y por qué podría ocurrir esta pérdida. Para ello se deben identificar: los activos, las amenazas, los controles existentes, las vulnerabilidades y las consecuencias.
  - Estimación del riesgo: una metodología de estimación puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias; en la práctica, con frecuencia se utiliza, en primer lugar, la estimación cualitativa para obtener una indicación general del nivel del riesgo y revelar los riesgos más importantes, y posteriormente, de ser necesario, se realiza un análisis cuantitativo de los riesgos importantes, dado que es, por lo general, menos complejo y menos costoso realizar un análisis cualitativo que uno cuantitativo.
  - Evaluación del riesgo: consiste en comparar los niveles de riesgo frente a los criterios para la evaluación del riesgo y sus criterios de aceptación.
- Tratamiento del riesgo: consiste en seleccionar controles para reducir, retener, evitar o transferir los riesgos; se debería definir un plan para tratamiento del riesgo.
- Aceptación del riesgo: consiste en tomar la decisión de aceptar los riesgos y las responsabilidades de la decisión, y registrarlo de manera formal.

CRAMM

Según Qasem (2013), el *CCTA[1] Risk Analysis and Management Method* [CRAMM] ofrece un enfoque por etapas, disciplinado, que abarca aspectos técnicos y no técnicos de seguridad; se divide en tres etapas:

1. *Central Communication and Telecommunication Agency*

Identificación de activos y valoración: identifica los activos físicos, el software y los datos que conforman el sistema de información y su ubicación. Los activos físicos se valoran en términos del costo de reposición; los activos de datos y software, en términos del impacto causado si la información no estuviera disponible, fuera destruida, divulgada o modificada.

Evaluación de amenazas y vulnerabilidades: consiste en identificar la probabilidad de que los problemas potenciales se produzcan. CRAMM cubre toda la gama de amenazas, deliberadas o accidentales, que pueden afectar a los sistemas de información.

Selección de contramedidas y recomendaciones: compara la evaluación de los riesgos con el nivel de seguridad requerido, con el fin identificar si los riesgos son lo suficientemente grandes como para justificar la instalación de una contramedida particular.

Magerit

En España, el Consejo Superior de Administración Electrónica (2012) estableció la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [Magerit] con el objetivo de implementar un marco común para el análisis y la gestión de riesgos en los sistemas de información, sobre la base de la norma ISO/IEC 27000. Esta metodología propone cuatro etapas:

- Etapa 1: planeación del análisis y la gestión de riesgos: establece las consideraciones necesarias para iniciar el análisis de riesgos y el proyecto de gestión, lo que permite investigar si es apropiado llevarlo a cabo.
- Etapa 2: análisis de riesgos: permite identificar y evaluar los elementos que intervienen en el riesgo para obtener una evaluación del riesgo en las diferentes áreas del dominio y estimar los umbrales de riesgo deseables.
- Etapa 3: gestión de riesgos: permite identificar las salvaguardias potenciales que reducen el riesgo detectado, simulando diferentes combinaciones de las mismas para especificar finalmente las seleccionadas.
- Etapa 4: selección de salvaguardias: permite seleccionar las contramedidas a implementarse, diseñando un enfoque para la aplicación de las salvaguardias seleccionadas. Establece los mecanismos para el seguimiento de su implementación, compila los documentos de trabajo para el análisis de riesgos y el proceso de gestión, obtiene los documentos finales del proyecto y presenta los resultados en los diferentes niveles.

Metodología del NIST para la gestión de riesgos para sistemas de TI

Esta guía del *National Institute of Standards and Technology* [NIST] proporciona las bases para el desarrollo de un programa de gestión de riesgos efectivo que contiene, tanto las definiciones, como las orientaciones prácticas necesarias para evaluar y mitigar los riesgos identificados dentro de los

CRAMM

According to Qasem (2013), the *CCTA' Risk Analysis and Management Method* [CRAMM] provides a phased approach that is disciplined, covering technical and non-technical security aspects. It is divided into three stages:

- Asset identification and assessment: Identifies the physical assets, software and data that comprise the information system and its location. Physical assets are valued in terms of replacement cost; data assets and software, in terms of the impact if the information is not available, was destroyed, disclosed, or modified.
- Assessment of threats and vulnerabilities: Consists in identifying the probability of potential problems occurring. CRAMM covers the entire range of threats, deliberate or accidental, that can affect information systems.
- The selection of countermeasures and recommendations: To compare the risk assessment with the level of security required to identify if the risks are large enough to justify the installation of a special countermeasure.

Magerit

In Spain, the Consejo Superior de Administración Electrónica (2012) established the methodology Analysis and Risk Management Information Systems [Magerit] with the objective of implementing a common framework for analysis and risk management of information systems, based on the ISO/IEC standard 27000. This methodology proposes four stages:

- Stage 1: Planning analysis and risk management: Establishes the necessary considerations to initiate risk analysis and project management, allowing investigation of whether it is appropriate to carry it out.
- Stage 2: Risk analysis: Allows the organization to identify and evaluate the factors involved in the risk, to obtain a risk assessment in different areas of the domain and estimate the desired risk thresholds.
- Stage 3: Risk management: Allows the organization to identify potential safeguards that reduce the risk identified, simulating different combinations thereof, to finally specify the selected option.
- Stage 4: Selection of safeguards: allows selection of countermeasures to be implemented, designing an approach to the application of the selected safeguards. It establishes mechanisms to monitor its implementation, compiles the work documents for risk analysis, and the management process, produces the final project documents, and presents the results at different levels.

NIST Risk Management Methodology for IT systems

This guide by the National Institute of Standards and Technology [NIST] provides the basis for the development of an effective program of risk management, containing both the definitions and the practical guidelines needed to assess and mitigate the risks identified within IT systems. This guide has nine well-defined steps (NIST, 2001):

- Step 1: Characterization of the system: identifies the boundaries of the IT system together with the resources and information that constitute it.
- Step 2: Identification of threats: identifies the threats that can affect the IT system; to determine the probability of a threat, the sources of threats, potential vulnerabilities and existing controls can be considered.
- Step 3: Identification of vulnerabilities: creates a list of vulnerabilities –flaws or weaknesses– of the system, which can be exploited by potential sources of threat.
- Step 4: Analysis of controls: analyzes the implemented controls, or those which the organization plans to implement, whether they are for prevention –to prevent attempts to violate security policies and including execution control, encryption and authentication– or detection – that warn of violations or attempted violations of security policies, and include audits of tracking, intrusion detection methods and error control.
- Step 5: Determination of probability: to obtain the probability that a potential vulnerability can be exploited by an associated threat, the following factors can be considered: motivation and capability of the source of threat, the nature of the vulnerability and the existence and effectiveness of current controls.
- Step 6: Impact analysis: consists of measuring the level of risk to determine the adverse impact resulting from the successful exploitation of a vulnerability by a threat; the adverse impact on a security system can be described in terms of the loss or degradation of one or a combination of the following security objectives: integrity, availability and confidentiality.
- Step 7: Risk assessment: consists of evaluating the risk level of the IT system; risk assessment for a particular threat/vulnerability pair can be expressed in terms of: the probability that an attempted threat can exploit a particular vulnerability; the magnitude of the impact when a threat successfully exploits a vulnerability; and the adequacy of security controls, planned or existing, to reduce or elimi-

sistemas de TI (Tecnologías de Información). Esta guía tiene nueve pasos definidos así (NIST, 2001):

- Paso 1: caracterización del sistema: identifica los límites del sistema TI, junto con los recursos y la información que lo constituyen.
- Paso 2: identificación de amenazas: identifica las amenazas que pueden afectar el sistema TI; para determinar la probabilidad de una amenaza, se pueden considerar las fuentes de amenaza, las vulnerabilidades potenciales y los controles existentes.
- Paso 3: identificación de vulnerabilidades: crea una lista de las vulnerabilidades –fallas o debilidades– del sistema, que pueden ser explotadas por las fuentes potenciales de amenaza.
- Paso 4: análisis de controles: analiza los controles implementados o que planea implementar la organización, sean preventivos –que evitan los intentos de violar las políticas de seguridad e incluyen el control de ejecución, el cifrado y la autenticación– o de detección –que alertan sobre violaciones o intentos de violaciones de las políticas de seguridad e incluyen auditorías de rastreo, métodos de detección de intrusión y control de errores–.
- Paso 5: determinación de la probabilidad: para obtener la probabilidad de que una vulnerabilidad potencial pueda ser explotada por una amenaza asociada, se pueden considerar los siguientes factores: motivación y capacidad de la fuente de amenaza, naturaleza de la vulnerabilidad, y existencia y efectividad de los controles actuales
- Paso 6: análisis del impacto: consiste en medir el nivel de riesgo para determinar el impacto adverso que resulta de la explotación exitosa de una vulnerabilidad por una amenaza; el impacto adverso de un sistema de seguridad puede describirse en términos de la pérdida o degradación de uno o de una combinación de los siguientes objetivos de seguridad: integridad, disponibilidad y confidencialidad.
- Paso 7: determinación de riesgos: consiste en evaluar el nivel de riesgo del sistema TI; la determinación del riesgo para una pareja particular amenaza/vulnerabilidad puede ser expresada en función de: la probabilidad de que un intento de amenaza dado explote una determinada vulnerabilidad; la magnitud del impacto cuando una amenaza explota exitosamente una vulnerabilidad; y la idoneidad de los controles de seguridad planeados o existentes para reducir o eliminar los riesgos. Se debe obtener: la medida del riesgo, la escala del riesgo y la matriz de nivel del riesgo.
- Paso 8: recomendaciones de control: determina los controles que pueden mitigar o eliminar los riesgos identificados. Los siguientes factores deberían considerarse al recomendar controles: efectividad de las opcio-

nes recomendadas (es decir, compatibilidad del sistema), legislación y regulación, política organizacional, impacto operacional, y seguridad y confiabilidad.

- Paso 9: documentación de resultados: Los resultados deben ser documentados en un reporte oficial o instrucciones; un reporte de evaluación de riesgos es un reporte de gestión que ayuda a la alta gerencia a tomar decisiones respecto de las políticas, los procedimientos, el presupuesto y los cambios en el sistema operacional y de gestión.

Metodología del BID para el diagnóstico, la prevención y el control de la corrupción en programas de seguridad ciudadana

Esta metodología parte de la correlación entre la seguridad ciudadana y la corrupción, y se basa en el análisis de la cadena de valor; se identifican los procesos que aportan más a la generación de valor en una organización o programa, para lo cual se dividen en dos tipos: actividades primarias o críticas –que contribuyen directamente a la creación de valor–, y actividades administrativas o de soporte –que sustentan el desarrollo de las actividades primarias–.

Los macro-procesos críticos de la cadena de valor de la seguridad ciudadana son (García-Mejía, 2010):

- Desarrollar políticas de seguridad: articular la respuesta pública a las demandas y necesidades sociales de seguridad ciudadana.
- Prevenir la violencia: contrarrestar los factores multidimensionales que aumentan los riesgos de criminalidad y victimización.
- Controlar y sancionar: asegurar el respeto de la ley y el orden público, proteger a las personas y bienes ante la amenaza de delitos, de ser el caso, aplicando las consecuencias jurídicas derivadas del incumplimiento de la ley.
- Rehabilitar y reinsertar en la sociedad: tratar y rehabilitar a la población reclusa o a menores de edad que han infringido la ley (prevención terciaria) para su reinserción social, así como a las víctimas de delitos.
- Supervisar y evaluar las políticas: monitorear, supervisar y evaluar el cumplimiento de la misión, los objetivos y las metas establecidas en los planes y actividades de manera ordenada y eficiente.

Cada uno de estos macro-procesos implica llevar a cabo los siguientes pasos (García-Mejía, 2010):

- Identificación y análisis de los riesgos: identificar los riesgos de cada uno de los principales procesos, así como su nivel, entendido éste como la probabilidad de ocurrencia y el impacto que generaría en caso de materializarse; el impacto del riesgo varía en cada proyecto, por lo que debe ser analizado, caso por caso.
- Respuesta a los riesgos: identificar un abanico de alternativas de respuesta a los riesgos identificados; se puede

nate risks. The risk measure, the scale of risk and level of risk matrix must be obtained.

- Step 8: Control recommendations: determines the controls that can mitigate or eliminate the identified risks. For the recommendation of controls the following controls should be considered: effectiveness of the recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability.
- Step 9: Documentation of results: results should be documented in an official report or instructions; a risk assessment report is a management report that helps senior management to make decisions on policies, procedures, budget and changes in the operational and management system.

IDB Corruption Diagnosis, Prevention and Control in Programs of Civic Security Methodology

This methodology is based on the correlation between citizens' security and corruption, and on the analysis of the value chain; the processes that contribute most to the generation of value in an organization or program are identified, and divided into two types: critical or primary activities –that contribute directly to the creation of value–, and administrative activities or support –supporting the development of primary activities.

The critical macro-processes of the value chain of public safety are (García-Mejía, 2010):

- Develop security policies: Orchestrating the public response to the demands and social needs of public safety.
- Violence prevention: Counteract the multi-dimensional factors that increase the risk of crime and victimization.
- Control and sanction: Ensure compliance with the law and public order, protect people and assets against the threat of crime, applying, if appropriate, the juridical consequences due to breach of law.
- Rehabilitate and reintegrate into society: Treat and rehabilitate the prison population or minors who have infringed the law (tertiary prevention) for their social reintegration, as well as victims of crime.
- Monitor and evaluate policies: Monitor, supervise, and evaluate the achievement of the mission, objectives and goals set in plans and activities in an orderly and efficient manner.

Each of these macro-processes involves performing the following steps (García-Mejía, 2010):

- Identification and analysis of risks: To identify the risks of each of the main processes as well as its level, understand this as the probability of occurrence and the impact that would be generated if it is materialized; the impact of risk on each project varies, and should therefore be analyzed case by case.
- Risk response: Identifying a range of possible responses to the identified risks; one or a combination of actions able to give an effective response to the identified risks can be selected; to accomplish this response to the risks, consideration is given to the dimensions of analysis and a review of the available alternatives.

Two dimensions of analysis were taken into account: The risk responses that can be transversal and specific, and strategic categories of risk response suggested by the Project Management Institute [PMI] (2008), mainly to avoid and mitigate.

In some cases, the risk responses are generated by reforms to other processes of the value chain, and not directly to the process at risk, since the source of risk is another process.

Concerning the review of the available alternatives, the fight against corruption can be not only or primarily an effort to identify and punish the corrupt, which in any case is necessary and essential, but to identify patterns of corruption, that is, the most vulnerable areas, and its main manifestations, in order to modernize institutional management to reduce the individual discretion of public servants, make their actions transparent and hold them accountable for their acts (Campos & Pradhan, 2007).

NIST Malware Incident Prevention Methodology

In this methodology, the NIST considers that the four main elements of prevention are (Mell et al., 2005):

- Policies: Policies aimed at preventing malware are the basis for implementing preventive controls. If an organization does not clearly establish malware prevention considerations into their policies, it is improbable that they will be able to perform malware prevention activities consistently and effectively along the organization. Policies related to malware prevention should be as wide as possible to provide flexibility in their implementation and reduce the need for frequent updates, as well as being sufficiently specific in order that their purpose and scope are clear.
- Awareness: Establish and maintain general programs of raising awareness about malware for all users, as well as specific training programs about raising awareness for IT staff directly involved in incident prevention activities, this being critical to reduce the number of incidents that occur

seleccionar una o una combinación de acciones capaz de dar una respuesta efectiva a los riesgos identificados; para llevar a cabo esta respuesta a los riesgos se consideran: las dimensiones de análisis y la revisión de las alternativas disponibles.

Se tuvo en cuenta dos dimensiones de análisis: las respuestas a los riesgos, que pueden ser transversales y específicas, y las categorías estratégicas de respuesta a los riesgos sugeridas por el Project Management Institute [PMI] (2008), principalmente evitar y mitigar.

En algunos casos las respuestas a los riesgos pasan por introducir reformas a otros procesos de la cadena de valor, no directamente al proceso en riesgo, pues el origen del riesgo está en otro proceso.

En cuanto a la revisión de las alternativas disponibles, la lucha contra la corrupción no puede ser solo ni principalmente un esfuerzo para identificar y castigar a los corruptos, lo que en cualquier caso es necesario e imprescindible, sino por identificar los patrones de la corrupción, esto es, sus áreas más vulnerables y sus principales manifestaciones, con el propósito de modernizar la gestión institucional para reducir la discrecionalidad de los servidores públicos, transparentar su actuación y hacerlos responsables de sus actos (Campos & Pradhan, 2007).

Metodología de prevención de incidentes de malware del NIST

En esta metodología, el NIST considera que los cuatro elementos principales de la prevención son (Mell et al., 2005):

- Políticas: las políticas dirigidas a la prevención del malware son la base para implementar controles preventivos. Si una organización no establece claramente las consideraciones de prevención del malware en sus políticas, es improbable que lleve a cabo actividades de prevención del malware consistentes y efectivas a lo largo de la organización. Las políticas relacionadas con la prevención del malware deben ser tan generales como sea posible para proveer flexibilidad en su implementación y reducir la necesidad de frecuentes actualizaciones de las mismas, pero también deben ser lo suficientemente específicas para que su propósito y alcance sean claros.
- Concientización: establecer y mantener programas generales de concientización sobre el malware para todos los usuarios, así como programas de entrenamiento específico en concientización para el personal de TI directamente involucrado en las actividades de prevención de incidentes, es crítico para reducir el número de incidentes que ocurre por errores humanos. Todos los usuarios de una organización deberían ser conscientes de: las maneras en que entra el malware a los sistemas, los infecta y se expande; los riesgos que supone el malware; la inhabilidad de los controles técnicos para prevenir todos los incidentes y la importancia de que los usuarios prevengan estos incidentes.

- Mitigación de vulnerabilidades: invertir esfuerzos en la mitigación de vulnerabilidades puede eliminar algunos posibles vectores de ataque. Debido a los desafíos que presenta la mitigación de vulnerabilidades, incluyendo el continuo descubrimiento de nuevas vulnerabilidades, las organizaciones deben tener documentadas las políticas, los procesos y los procedimientos para la mitigación de vulnerabilidades, y deberían también considerar la creación de un programa de gestión de vulnerabilidades que ayude en las tareas de mitigación. También se deben evaluar constantemente las vulnerabilidades, para que las tareas de mitigación sean priorizadas apropiadamente.
- Mitigación de amenazas: implementar una combinación de técnicas y herramientas de mitigación de amenazas, como software antivirus y cortafuegos, puede prevenir las amenazas que atacan exitosamente los diferentes sistemas y redes. Las organizaciones deben realizar la mitigación de amenazas para detectar y parar el malware antes de que afecte a sus objetivos.

Las organizaciones deben crear una guía de recomendaciones para cada categoría a fin de crear una defensa en capas efectiva contra el malware. Sin embargo, las organizaciones deben ser conscientes de que, sin importar el esfuerzo que pongan en la prevención de incidentes de malware, los incidentes aún ocurrirán –por ejemplo, por tipos de amenaza desconocidos, errores humanos, etc.– (Mell et al., 2005).

IV. Aspectos a comparar

Ya que se van a comparar diferentes metodologías, se va a establecer un paralelo entre las fases o pasos que estas incluyen. Se han identificado cuatro fases básicas, que se repiten en casi todas ellas:

- Establecer el contexto: identificar los activos importantes para la organización, los requisitos de seguridad de esos activos, lo que la organización está haciendo para protegerlos, y los objetivos que se persiguen con el análisis de riesgos.
- Identificar los riesgos: determinar qué vulnerabilidades poseen los diferentes activos e identificar las amenazas que pueden explotarlas.
- Analizar los riesgos: calcular la probabilidad de que una amenaza explote una determinada vulnerabilidad y establecer el nivel de riesgo de cada activo, priorizándolos para tomar acciones posteriores.
- Tratar los riesgos: implantar contramedidas que permitan evitar, mitigar, aceptar o transferir los riesgos.

La comparación va a consistir en determinar si las diferentes metodologías incluyen estas fases y establecer si se enfocan en una fase determinada o si especifican claramente lo que se hace en cada una de ellas. También se va a determinar si estas metodologías consideran el factor humano dentro de sus diferentes pasos, ya que el ser humano es el eslabón más débil de la cadena de la seguridad.

due to human error. All users in an organization should be conscious of the ways in which malware enters, infects and expands in systems; the risks involved in malware; the inability of technical controls to prevent all incidents, and the importance of users avoiding such incidents.

- Vulnerabilities mitigation: Investing efforts in the mitigation of vulnerabilities can eliminate some possible attack vectors. Due to the challenges posed by mitigating vulnerabilities, including the continual discovery of new vulnerabilities, organizations must have documented policies, processes and procedures for mitigating vulnerabilities, and they should also consider creating a vulnerability management program to assist in the mitigation tasks. Also, vulnerabilities must be constantly evaluated, in order that mitigation tasks are prioritized appropriately.
- Threat mitigation: Implementing a combination of techniques and threat mitigation tools, such as antivirus software and firewalls, can successfully prevent threats that attack the different systems and networks. Organizations should perform threat mitigation to detect and stop malware before it affects their objectives.

Organizations must create a guide with recommendations for each category in order to create an effective layered defense against malware. However, organizations should be aware that, regardless of the effort put into preventing malware incidents, incidents will still take place – for example, by unknown types of threats, human error, etc. (Mell et al., 2005).

IV. Aspects to compare

Since different methodologies will be compared, a comparison between the phases or steps that include these should be established. Four basic steps that are repeated in almost all of them have been identified:

- Set the context: Identify important assets for the organization, the security requirements of these assets, what the organization is doing to protect them, and the objectives pursued with risk analysis.
- Identify risks: Determine which vulnerabilities the different assets have and identify threats that can exploit them.
- Analyze risks: Calculate the probability that a threat will exploit a particular vulnerability and establish the level of risk of each asset, and prioritize them for taking action in response.
- Deal with risks: Implement countermeasures to avoid, mitigate, accept or transfer risks.

Metodología...	De gestión de riesgos							De Prevención de Riesgos	
Ítem	OCTAVE (Phases)	CORAS (Steps)	Australian St (Phases)	NTC – ISO/ IEC 27005 (Steps)	CRAMM (Stages)	MAGERIT (Stages)	NITS (Steps)	BID (Steps)	NIST (core elements)
Establishment of the context/ Establecer el contexto	1	1, 2, 3	1	1	1	1	1	N/A	N/A
Identify risks/ Identificar los riesgos	1 y 2	4	2	2	2	2	2, 3, 4	1	N/A
Analyze risks/ Analizar los riesgos	3	5 y 6	3 y 4				5, 6, 7		N/A
Manage risks/ Tratar los riesgos		7	5	3 y 4	3	3 y 4	8 y 9	2	4

Table 2. Comparison of methodologies / Comparación de metodologías

The comparison will be to determine whether the different methodologies include these phases and establish if they focus on a particular stage or if they specify clearly what is done in each one; also to determine whether these methodologies consider the human factor in the different steps, since the human being is the weakest link in the security chain.

V. Comparison of Methodologies

Table 2 compares the different methodologies described, indicating whether they include the phases identified in section IV of this article.

As shown in Table 2, the Octave methodology, while including the four phases that are defined for this analysis, does not present a strict division of them. Octave focuses mainly on the first phase, where the knowledge and safety practices of senior management, operational and staff are identified, and so builds the different profiles of threats; therefore, at this stage it takes into account the human factor. Risk identification is carried out in the first and second phases of Octave, because in the first phase it establishes the threats profiles and in the second identifies vulnerabilities. However, to determine in the first instance the threats and then the vulnerabilities, the correspondence between these is not clear, given that the identification of which threats can exploit a particular vulnerability must be done; at this stage of risks identification, the human factor is not explicitly considered, but rather the assets of the organization. The third phase of Octave includes both the analysis and treatment of risks and takes into account the human factor, because in its processes it includes risk analysis of behavior and promotes the protection strategy in the organization. However, specific protection and prevention strategies are not established.

The CORAS methodology is based on the realization of a series of meetings and workshops for different purposes, according to the step that is being performed. As shown in Table 2, this

V. Comparación de metodologías

En la Tabla 2 se muestra el cuadro comparativo de las diferentes metodologías descritas, indicando si incluyen las fases identificadas en la sección IV de este artículo.

Como se puede apreciar en la Tabla 2, la metodología Octave, aunque incluye las cuatro fases que se han definido para este análisis, no presenta una división estricta de ellas. Octave se centra principalmente en su primera fase, donde se identifica primero el conocimiento y prácticas de seguridad de la alta gerencia, del área operacional y del personal, para construir posteriormente los diferentes perfiles de amenazas; por tanto, en esta fase se tiene en cuenta el factor humano. La identificación de riesgos, se lleva a cabo en la primera y segunda fase de Octave, porque en la primera fase establece los perfiles de amenazas y en la segunda identifica las vulnerabilidades, sin embargo, al determinar primero las amenazas y luego las vulnerabilidades, no queda claro la correspondencia entre estas, pues se debe identificar qué amenazas pueden explotar una determinada vulnerabilidad; en esta fase de identificación de los riesgos no se considera explícitamente el factor humano sino los activos de la organización. La tercera fase de Octave incluye, tanto el análisis, como el tratamiento de los riesgos, y tiene en cuenta el factor humano, porque en sus procesos hace un análisis de riesgos de conducta y fomenta la estrategia de protección en la organización, sin embargo, no se establecen estrategias específicas de protección y prevención.

En cuanto a la metodología CORAS, esta se basa en la realización de una serie de reuniones y talleres con diferentes fines, de acuerdo con el paso que se esté realizando. Como se aprecia en la Tabla 2, esta metodología incluye las cuatro fases consideradas en este análisis. La fase de establecimiento del contexto, se lleva a cabo en los tres primeros pasos de CORAS, en este caso, los analistas se basan en la información proporcionada por los representantes del cliente, por lo que no son ellos los que reúnen directamente la información que requieren de la empresa, lo que puede llevar a no contar con toda la información necesaria para realizar un análisis de riesgos completo; sin embargo, se hacen en

esta primera fase tres reuniones para asegurar la completa y adecuada comprensión de la información presentada por el cliente. La fase de identificación de riesgos, se lleva a cabo en el cuarto paso, donde se identifican las vulnerabilidades y los diferentes escenarios de amenaza a través de un taller con expertos en el objeto de análisis. La fase de análisis de riesgos, se lleva a cabo en los pasos 5 y 6, donde se obtienen los valores de probabilidad y un cuadro de riesgos general. La fase de tratamiento de riesgos, se lleva a cabo en el séptimo paso, donde se determina qué tratamiento se va a dar a los riesgos y se hace un análisis costo/beneficio. Ya que los analistas no tienen un contacto directo con el personal de la empresa cliente, esto puede llevar a descuidar el factor humano y a tener una visión errada de los procesos y de las prácticas de seguridad que se llevan a cabo en ella, obteniendo resultados que pueden no adaptarse al contexto real de la empresa. No se establecen estrategias específicas de protección y prevención.

Según la TABLA 2, la metodología de administración de riesgos del estándar australiano incluye las cuatro fases consideradas en este análisis. Esta metodología se centra en las fases de identificación y análisis de riesgos, donde se incluyen todos los riesgos (estén o no bajo el control de la organización) y se analizan las fuentes y consecuencias de los mismos para calcular luego su probabilidad y establecer su nivel, de acuerdo con un análisis, tanto cualitativo, como cuantitativo. Sin embargo, el establecimiento del contexto se hace teniendo en cuenta el contexto estratégico, organizacional y de administración de riesgos, por lo que no se centra en el factor humano, sino en los objetivos que quiere alcanzar la organización; tampoco se definen estrategias específicas de protección y prevención en la fase de tratamiento de los riesgos, aunque sí se establece un proceso cíclico de tratamiento de los mismos, lo que permite verificar si las contramedidas implementadas tienen el efecto esperado o si deben reemplazarse por otras.

La metodología de gestión de riesgos NTC-ISO /IEC 27005 incluye las cuatro fases consideradas en este análisis, pero no menciona específicamente el factor humano, pues sus pasos se describen de manera muy general. Esta metodología tiene un interés particular en la valoración del riesgo donde se realiza la identificación, estimación y evaluación del mismo.; ya que la eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo, si la información que arroja este paso no es suficiente, se llevan a cabo tantas iteraciones como sean necesarias de valoración del riesgo con un contexto revisado, para poder realizar un tratamiento adecuado. Además, no se definen estrategias específicas de protección y prevención en el paso de tratamiento del riesgo.

El método de análisis CRAMM, aunque incluye las cuatro fases consideradas en este análisis, es bastante general y no se centra en ninguna de estas fases; tampoco habla específicamente del factor humano ni define estrategias específicas de protección y prevención. La etapa de identifi-

methodology includes the four phases considered in this analysis. The phase of establishing the context takes place in the first three steps of CORAS. In this case, analysts depend on information provided by representatives of the customer, so they do not directly gather the information required from the company, which may mean that not all the information necessary to perform a full risk analysis is available. However, three meetings are held in this first phase to ensure full and proper understanding of the information presented by the client. The risk identification phase is carried out in the fourth step, where different vulnerabilities and threat scenarios are identified, through a workshop with experts on the object of analysis. The risk analysis phase is carried out in steps 5 and 6, where the probability values and a picture of the overall risk are obtained. The phase of risk treatment is carried out in the seventh step, where it is determined how the risks will be handled, and a cost/benefit analysis is performed. Since the analysts have no direct contact with the staff of the client company, this can lead to neglect of the human factor and a mistaken view of the processes and safety practices that are carried out, yielding results that are possibly not related with the actual context of the company. No specific protection and prevention strategies are set.

According to TABLE 2, the risk management methodology of the Australian Standard includes the four phases considered in this analysis. This methodology focuses on the phases of identification and risk analysis, where all risks are included (whether or not under the control of the organization) and the sources and consequences of these are analyzed, after which the probability is calculated, and their levels are established, according to an analysis in both qualitative and quantitative terms. However, the establishment of the context is performed according to the strategic, organizational and risk management context, so it does not focus on the human factor, but rather on the objectives that the organization wants to achieve. The treatment phase of the risks does not define specific strategies for protection and prevention, even if a cyclical process of treatment of the same is established, and thus does not allow a verification that the implemented countermeasures have the desired effect or whether they should be replaced by others.

The risk management methodology NTC-ISO / IEC 27005 includes the four phases considered in this analysis, but does not specifically mention the human factor, because the steps are described in very general terms. This methodology is particularly interested in the risk assessment, with identification, estimation and evaluation of the risk; since the efficacy of the risk treatment depends on the results of the risk assessment, if the information obtained in this step is not sufficient, iterations are carried out as

necessary of the risk assessment with a revised context, to ensure appropriate treatment. In addition, no specific protection and prevention strategies are defined in the risk treatment step.

The CRAMM analysis method, though including the four phases considered in this analysis, is rather general and does not focus on any of these phases, and does not speak specifically of the human factor or define specific strategies for protection and prevention. The asset identification and evaluation stage of CRAMM focuses only on physical assets and information, although at the stage of assessing threats and vulnerabilities it affirms that all deliberate and accidental threats are considered, which could imply the human factor.

The Magerit methodology is also very general in the description of its stages, though it includes the four phases considered in this analysis. In the planning stage of analysis and risk management it does consider human resources, but in carrying out risk analysis it does not speak of the human factor in the organization. In addition, in the analysis stage of risk it does not specify what types of threat are considered, or the process of identifying desirable risk thresholds. Magerit focuses mainly on the stage of risk management which simulates different combinations of safeguards in order to select those that best fit the context of the organization, and then, at the stage of selecting safeguards, monitors the implementation of these safeguards, documenting and disclosing them at different levels of the organization. Thus, at least at this stage, it takes into account the human factor. Magerit does not define specific strategies for protection and prevention.

The NIST methodology of risk management is perhaps the most complete methodology of all those studied, because it includes the four phases considered in this analysis and provides definitions such as the practical guidance needed to assess and mitigate the risks identified in IT systems, and consequently describes in a very precise way what to do in each of its nine steps. This methodology also considers the human factor, taking into account the motivation of the different sources of threats, which helps determine the likelihood of risk. It also considers preventive and corrective controls.

Methodologies for risk prevention provide an overview focused on risk analysis and especially on the treatment of these same risks. The IDB methodology for the diagnosis, prevention and control of corruption in citizen security programs, although not oriented to IT systems, is very interesting for this study because it focuses on the human factor, considering the chain value of the different processes that are carried out in an organization, as well as the individual, institutional and social responsibilities at the time of implementing preventive controls. In this methodology the identification and analysis of risk is performed mainly in

cación de activos y valoración de CRAMM se centra solo en los activos físicos y de información, aunque en la etapa de evaluación de amenazas y vulnerabilidades sí dice que se consideran todas las amenazas deliberadas o accidentales, lo que podría tener implícito el factor humano.

La metodología Magerit es también bastante general en la descripción de sus etapas, aunque incluye las cuatro fases consideradas en este análisis. En la etapa de planeación del análisis y gestión de riesgos considera los recursos humanos pero para llevar a cabo el análisis de riesgos, no habla en sí del factor humano de la organización. Además, en la etapa de análisis de riesgos no se especifica qué tipos de amenaza se consideran ni cómo se determinan los umbrales de riesgo deseables. Magerit se centra principalmente en la etapa de gestión de riesgos donde simula diferentes combinaciones de salvaguardias para seleccionar las que más se acomoden al contexto de la organización, y luego, en la etapa de selección de salvaguardias, hace un seguimiento a la implementación de estas salvaguardias, las documenta y las da a conocer en los diferentes niveles de la organización, así que, por lo menos en esta etapa, tiene en cuenta el factor humano. Magerit no define estrategias específicas de protección y prevención.

La metodología de gestión de riesgos del NIST es quizás la metodología más completa de todas las estudiadas, ya que incluye las cuatro fases consideradas en este análisis y proporciona, tanto las definiciones, como las orientaciones prácticas necesarias para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI, por lo que describe de una manera muy precisa lo que se debe hacer en cada uno de sus nueve pasos. Esta metodología también considera el factor humano, pues tiene en cuenta la motivación de las diferentes fuentes de amenazas, lo que ayuda a determinar la probabilidad del riesgo; además, considera los controles preventivos y correctivos.

Las metodologías de prevención de riesgos ofrecen un panorama centrado en el análisis de riesgos y sobretodo en el tratamiento de los mismos. La metodología para el diagnóstico, prevención y control de la corrupción en programas de seguridad ciudadana del BID, aunque no es una metodología orientada a los sistemas de TI, es muy interesante para este estudio, pues se centra en el factor humano, considerando la cadena de valor de los diferentes procesos que se llevan a cabo en una organización y las responsabilidades individuales, institucionales y sociales, a la hora de implementar los controles preventivos. En esta metodología la identificación y el análisis de los riesgos se hacen de manera más cualitativa que cuantitativa, mientras en la respuesta a los riesgos se consideran varias dimensiones de análisis y se revisan las alternativas disponibles.

La metodología de prevención de incidentes de malware del NIST, por su parte, incluye solamente la fase del tratamiento de los riesgos, estableciendo los cuatro elementos principales de la prevención: las políticas, la concientización, la mitigación de vulnerabilidades y la mitigación de

amenazas. En la concientización es donde incluye el factor humano, y describe los aspectos a tener en cuenta para implementar los cuatro elementos de prevención.

IV. Conclusiones

De las siete metodologías de gestión de riesgos estudiadas, solo tres consideran el factor humano (Octave, Magerit y la metodología de gestión de riesgos del NIST) y cuatro no lo consideran de manera explícita (CORAS, la metodología del estándar australiano, la NTC-ISO/IEC 27005 y CRAMM). Por su parte, las metodologías de prevención de riesgos estudiadas sí consideran el factor humano, principalmente la de diagnóstico, prevención y control de la corrupción en programas de seguridad ciudadana del BID. Como se determinó en la introducción de este artículo, el que estas metodologías consideren el factor humano es muy importante, pues son los seres humanos el eslabón más débil en la cadena de la seguridad.

De las metodologías de gestión de riesgos, la más completa es la metodología de gestión de riesgos del NIST, ya que incluye las cuatro fases consideradas en este análisis y proporciona las definiciones y orientaciones prácticas necesarias para evaluar y mitigar los riesgos identificados en los sistemas de TI. Sin embargo, sería bueno complementar el análisis de riesgos que realiza, teniendo en cuenta las responsabilidades individuales, institucionales y sociales, como lo hace la metodología citada del BID, lo que podría llevar a implementar estrategias de prevención más completas y efectivas.

Por otra parte, la Metodología de Prevención de Incidentes de Malware del NIST, especifica los cuatro elementos principales de la prevención, brindando una buena guía sobre los aspectos a considerar a la hora de implementar estrategias de prevención.

Aunque las metodologías de prevención de riesgos estudiadas no incluyen las cuatro fases consideradas en este análisis, sí sería bueno que lo hicieran, puesto que del establecimiento adecuado del contexto y del análisis completo de los riesgos existentes van a derivarse las diferentes estrategias de prevención a implantar.

Finalmente, se puede concluir que una metodología de prevención de riesgos completa debería combinar los aspectos destacables de las diferentes metodologías estudiadas. S&T

a qualitative rather than quantitative way, while in the response to the risks, several dimensions of analysis are considered, and the available alternatives are reviewed.

The NIST methodology of malware incident prevention, meanwhile, includes only the phase of risk treatment, establishing the four main elements of prevention: policies, awareness, mitigation of vulnerabilities and threat. It is in the awareness that the human factor is included, describing aspects to consider for implementing the four elements of prevention.

VI. Conclusions

Of the seven risk management methodologies studied, only three consider the human factor (Octave, Magerit, and the NIST's risk management methodology) and four do not consider it explicitly (CORAS, Australian Standard methodology, NTC ISO/IEC 27005 and CRAMM). Meanwhile, of the methodologies of risk prevention studied, the human factor is considered mainly in the diagnosis, prevention and control of corruption in the public safety programs of the IDB. As determined in the introduction to this article, the fact that these methodologies consider the human factor is very important because humans are the weakest link in the security chain.

Of the methodologies of risk management, the most complete is the NIST methodology because it includes the four phases considered in this analysis and provides the definitions and practical guidance needed to assess and mitigate the risks identified in IT systems. However, it would be good to complement the risk analysis performed by taking into account the individual, institutional and social responsibilities, as does the aforementioned IDB methodology, which could lead to prevention strategies that are more complete and effective.

On the other hand, the NIST methodology of malware incident prevention specifies the four main elements of prevention, providing a good guide on aspects to consider at the time of implementing prevention strategies.

Although the methodologies of risk prevention studied did not include the four phases considered in this analysis, it would be good to include these, because the appropriate establishment of context and comprehensive analysis of the risks will make it possible to derive different prevention strategies to be implemented.

Finally, we can conclude that a complete risk prevention methodology should combine the highlights of the different methodologies studied. S&T

References / Referencias

Alberts, C., & Dorofee, A. (2001). *An introduction to the octave method*. Pittsburg, PA: Carnegie Mellon University.

AS/NZS 4360:1999 -Estándar Australiano, Administración de Riesgos. (1999). Retrieved form: http://www.bcu.gub.uy/Acerca-de-BCU/Concursos/Est%C3%A1ndar%20Australiano_Adm_Riesgos.pdf

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision, 37*(5), 437- 444.

Baje, K. (2001). *A platform for risk analysis of security critical systems* (CORAS. IST-2000-25031). Oslo, Norway: Norsk_ Regnesentral.

Brantingham, P. J. & Faust, F. L. (1976). A conceptual model of crime prevention. *Crime and Delinquency, 22*(3), 284-296.

British Standards Institution (BSI). (1991). *Quality vocabulary* (No. BS4778 (Part 3 Section 3.2 = IEC 1990 50(191)). London, UK: BSI.

British Standards Institution (BSI). (1999). BS7799-2. *Information security management -part 2: specification for information security management systems*. London, UK: BSI.

Campos, E. & Pradhan, S. (2007). *The many faces of the corruption: tracking vulnerabilities at the sector level*. Washington DC: World Bank.

Carnegie Corporation. (1997). *Carnegie Commission on Preventing Deadly Conflict. Final report with executive summary*. New York, NY: Carnegie Corporation.

Concha-EastMan, A. (2004). Violencia urbana en América Latina y el Caribe: dimensiones, explicaciones, acciones. In S. Rotker (Ed.), *Ciudadanías del miedo* (pp. 39-53.). Caracas, Venezuela: Nutjaes.

Consejo Superior de Administración Electrónica (2012). *MAGERIT version 3. Metodología de análisis y gestión de riesgos de los sistemas de información*.. Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Díaz-Aguado, M. J., Martínez-Arias, R., & Martín-Seoane, G. (2004). Prevención de la violencia y lucha contra la exclusión desde la adolescencia. In *Volumen uno: La violencia entre iguales en la escuela y en el ocio. estudios comparativos e instrumentos de valuación*. Madrid, España: Instituto de la Juventud.

Douglas, M. (1990). Risk as a forensic resource. Daedalus, 119(4). *Retrieved from:* http://www.jstor.org/stable/20025383

Ekblom, P. (2003). *The conjunction of criminal opportunity: a framework for crime reduction*. London, UK: Home Office Crime and Policing Group.

Froedick, S. (1997). The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management, 6*(2), 165-177.

García-Mejía, M. (2010). *Metodología para el diagnóstico, prevención y control de la corrupción en programas de seguridad ciudadana* (No. Documento de Debate #IDB-DP-117). Washington, DC: Banco Interamericano de Desarrollo (BID).

García-Ospina, C. & Tobón-Correa, O. (2000). Promoción de la salud, prevención de la enfermedad, atención primaria en salud y plan de atención básica. ¿Qué los acerca? ¿Qué los separa? *Hacia Promoción de la Salud, 5*, 7-21.

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. *Computer & Security, 24*, 16-30.

Graham, J., & Bennett, T. (1995). *Crime prevention strategies in Europe and North America* (Vol. 28). Helsinki-New York: European Institute for Crime Prevention and Control.

Hayden, C., & Blaya, C. (2001). Violence et comportements agressifs dans les écoles anglaises. In E. Debarbieux & C. Blaya (Eds.), *La violence en milieu scolaire-3- dix approches en Europe* (pp. 43-70.). Paris, France: ESF.

Huerta, A. (2012, April 2). Introducción al análisis de riesgos - metodologías (II) [blog security artwork]. Retrieved from: http://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

ISO/IEC_TR_13335-1. (1996). *Information technology - guidelines for the management of it security - part 1: concepts and models for it security* (1st ed.). Geneva, Switzerland: ISO/IEC.

Kailay, M. P., & Jarratt, P. (1995). RAMeX: a prototype expert system for computer security analysis and management. *Computers and Security, 14*, 449-463.

Khan-Pathan, A.S. (2010). *The state of the art in intrusion prevention and detection*. Kuala Lumpur, Malaysia: CRC.

Kirkwood, A. S. (1994). Why do we worry when scientists say there is no risk? *Disaster Prevention and Management, 3*(2), 15- 22.

Knepper, P. (2007). *Criminology and social policy*. London, UK: Saja.

Martínez, F., & Ruiz, J. (2001). *Manual de gestión de riesgos sanitarios*: Madrid, Spain: Díaz De Santos.

Mell, P., Kent, K., & Nusbaum, J. (2005). *Guide to malware incident prevention and handling*. Gaithersburg, MD: NIST.

Moses, R. H. (1992). Risk analysis and management. In K. M. Jackson & J. Hruska (Eds.), *Computer security reference book*. Oxford, UK: Butterworth-Heinemann.

National Institute of Standards and Technology (NIST). (1995). *An introduction to computer security*. Washington DC: US Department of Commerce.

National Institute of Standards and Technology (NIST). (2001). *Risk management guide for information technology systems*. Washington DC: US Department of Commerce.

NTC-ISO/IEC 27005: Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la Información. Bogotá, Colombia: ICONTEC.

Owens, S. (1998). *Information security management: an introduction*. London, UK: British Standards Institution.

Peyre, V. (1986). Introduction: elements d'un debat sur la prevention de la delinquance. *Annales de Vaucresson, 1*(24), 9-13.

Piper, S. (2011). *Intrusion detection systems for dummies*. Hoboken, NJ: Wiley.

Project Management Institute (PMI). (2008). *A guide to the project management body of knowledge (PMBOK Guide)* (4th ed.). Newtown Square, PA: PMI.

Qasem, M. (2013). Information technology risk assessment methodologies: current status and future directions. *International Journal of Scientific & Engineering Research, 4*(12), 966-972.

Rajmojnino, N., FradJi, D., Soldini, F., & Venjès, P. (1997). L'École comme dispositive simbolique et les violences: le exemple de trois ecoles em Marseille. In B. Charlot & J. C. Émin (Eds.), *Violences à l'école - État des Savoirs*. Paris, France: Masson & Armand Colin.

Royal Society. (1992). *Risk: analysis, perception and management*. London, UK: The Royal Society.

Sánchez-Peña, M., Sánchez-Delgado, K., Agudelo-Ramírez, A. (2015). Estrategias lúdicas para aumentar el conocimiento de un grupo de adolescentes escolarizados sobre la gingivitis. Duazary, 12(2), 100-111.

Savona, E. U. (2004). Ipotesi per uno scenario della prevenzione. In R. Selmini (Ed.), *La sura di la sicurezza urbana*, (pp. 273-284). Bologna, Italy: Il Mulino.

Sigerist, H. (1951). A history of medicine: primitive and archaic medicine. New York, NY: Oxford University Press.

Strutt, J. (1993). *Risk assessment and management: the engineering approach*. Cranfield, UK: Cranfield University.

Tonry, M. & Farrington, D. (1995). *Strategic approach to crime prevention. Crime and Justice, 19, 1-20. Retrieved from:* http://www.jstor.org/stable/1147594

Varjas, I., Villejas, O., Sánchez, A., & Holthuis, K. (2003). *Promoción, prevención y educación para la salud. San José, Costa Rica: EDNASSS. Available at:* http://www.cendeisss.sa.cr/paajrodca/modulos/Modulo2/Modulo_2.pdf

Walgrave, L., & De Coster, F. (1986). Une tentative de clarification de la notion de prévention. *Annales de Vaucresson, 1*(24), 31-51.

Wallensteen, P. & Möller, F. (2003). Conflict prevention: methodology for knowing the unknown (Uppsala Peace Research Papers No. 7, Department of Peace and Conflict Research). Sweden: Uppsala University. Retrieved from: http://www.pcr.uu.se/digitalAssets/61/61533_1prevention___knowing_the_unknown.pdf

Wallensteen, P. (2002). Understanding conflict resolution. London, UK: Saja.

Weiss, T. & Hubert, D. (2001). *The responsibility to protect* . Ottawa, ON: International Development Research Center. Available at: http://www.idrc.ca/EN/Resources/Publications/openebooks/963-1/index.html

Yu, E. (2004). Information systems (in the Internet age). In *Practical Handbook of Internet Computing*: Boca Raton, FL: CRC.

CURRICULUM VITAE

Nancy Acevedo Commercial and Systems Manager; Specialist in Project Management; and candidate to Magister in Informatics Project Management from Universidad de Pamplona (Colombia). Professor, OPS in the administrative area at the Basic Sciences Faculty, and member of LOGOS research group hotbed at the Universidad de Pamplona. / Administradora Comercial y de Sistemas, Especialista en Gerencia de Proyectos y candidata a Magister en Gestión de Proyectos Informáticos de la Universidad de Pamplona (Colombia). Se desempeña como docente hora cátedra, OPS en el área administrativa de la Facultad de Ciencias Básicas y miembro del semillero del grupo de investigación LOGOS de la Universidad de Pamplona.

Cristina Satizabal Electronics and Telecommunications Engineering from Universidad del Cauca (Colombia) and Ph.D in Telematics Engineering from Universidad Politécnica de Cataluña (España). Professor at the Telecommunications Engineering Program (Universidad de Pamplona) and member of the LOGOS research group. / Ingeniera en Electrónica y Telecomunicaciones de la Universidad del Cauca (Colombia) y Doctora en Ingeniería Telemática de la Universidad Politécnica de Cataluña (España). Se desempeña como docente de tiempo completo ocasional del Programa de Ingeniería en Telecomunicaciones de la Universidad de Pamplona, donde además forma parte del grupo de investigación LOGOS.

B. RESULTADOS DE ENCUESTAS A DOCENTES Y ESTUDIANTES

B.1 ENCUESTAS A DOCENTES

B.1.1 GÉNERO DE PARTICIPANTES

Tabla 37. Género de Participantes por Facultades

GÉNERO	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
Femenino	23	19	13	44	19	9	4
Masculino	13	48	30	40	35	10	10
Total	36	67	43	84	54	19	14

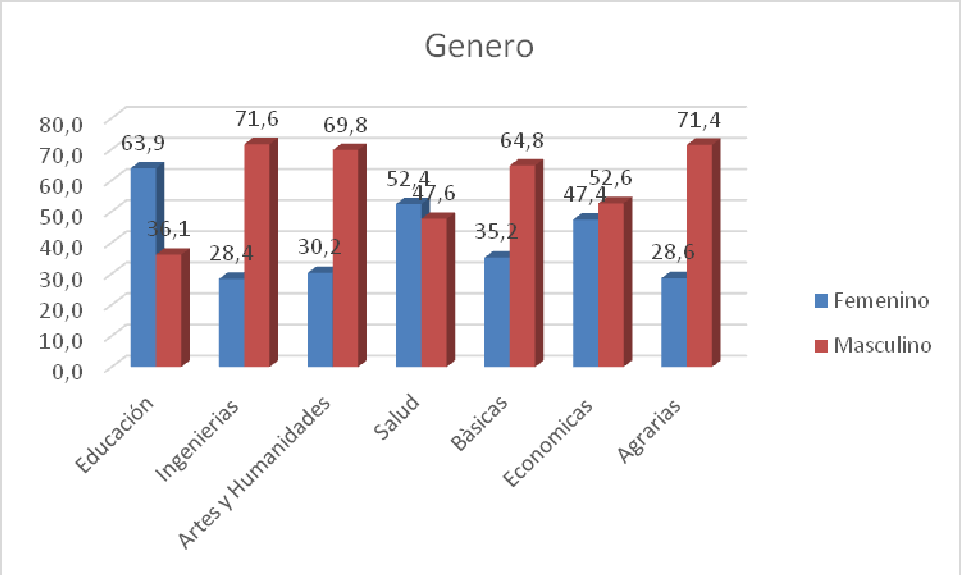

Figura 18. Porcentaje de Participantes por Género

B.1.2 PREGUNTA 1: ¿CUÁNTAS PERSONAS CONOCEN SU CONTRASEÑA DE INGRESO AL CAMPUS TI?

Esta pregunta cuenta con las siguientes opciones:

A. Solo usted
B. 2 personas
C. 3 personas o más

Tabla 38.Personas que Conocen Contraseña Campus TI por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	32	56	41	82	52	14	14
B	4	10	2	2	2	0	0
C	0	1	0	0	0	5	0

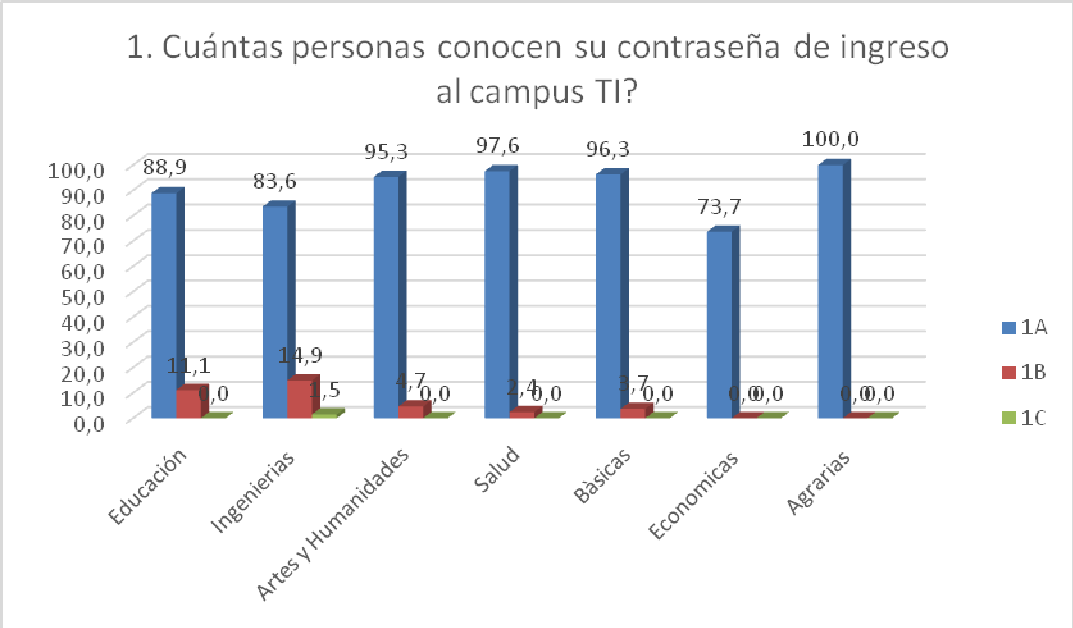

Figura 19. Porcentaje de Personas que Conocen Contraseña Campus TI

B.1.3 PREGUNTA 2: ¿LA LONGITUD DE SU CONTRASEÑA DE INGRESO AL CAMPUS TI?

Esta pregunta cuenta con las siguientes opciones:

A. 1 a 4 caracteres
B. 5 a 7 caracteres
C. 8 o más caracteres

Tabla 39. Longitud Contraseña Campus TI por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	8	0	0	0	0	5	2
B	28	28	22	55	28	0	8
C	0	39	21	29	26	14	4

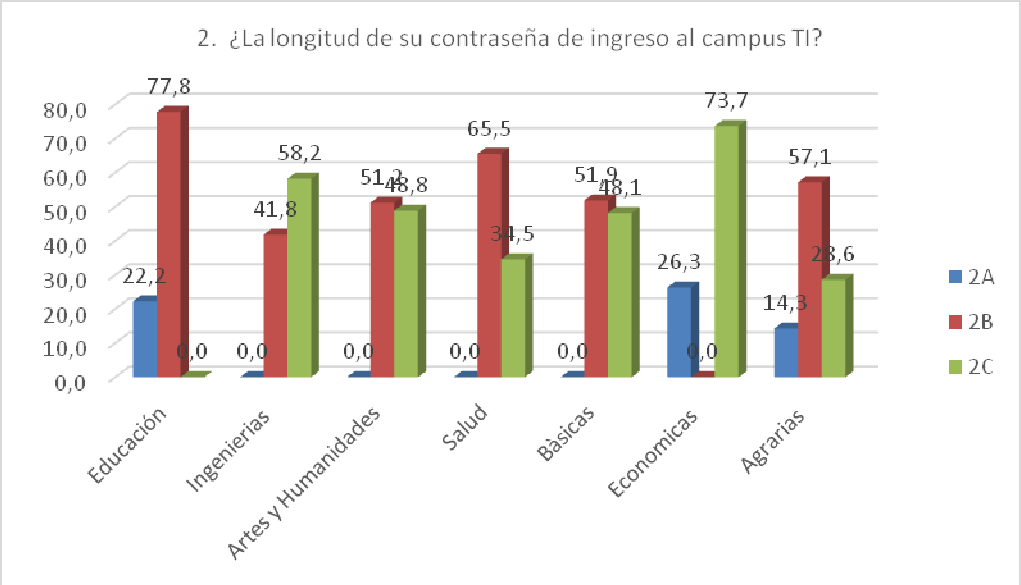

Figura 20. Porcentaje de Longitud de Contraseña Ingreso Campus TI

B.1.4 PREGUNTA 3: CUANDO ELIGE LA CONTRASEÑA DE INGRESO A SU CAMPUS TI

Esta pregunta cuenta con las siguientes opciones:

A. Prefiere una contraseña compleja y fácil de recordar.
B. Prefiere una contraseña compleja y difícil de recordar.
C. Prefiere una contraseña sencilla y fácil de recordar.
D. No le da importancia

Tabla 40. Complejidad Contraseña Campus TI por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	0	38	18	46	31	9	8
B	28	3	3	5	3	5	1
C	8	19	18	29	16	5	5
D	0	7	4	4	4	0	0

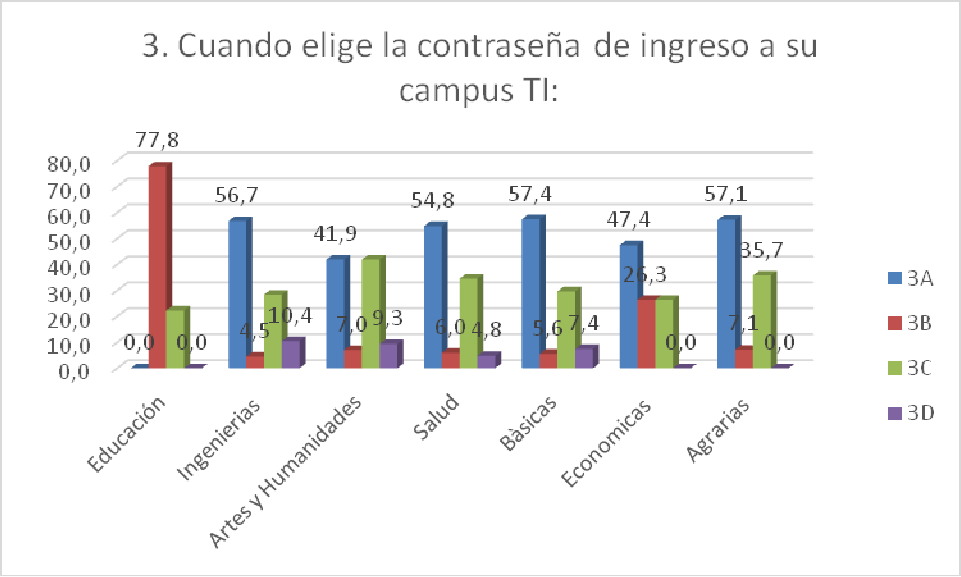

Figura 21. Porcentaje Complejidad Contraseña Campus TI

B.1.5 PREGUNTA 4: ¿CONOCE LAS POLÍTICAS DE SEGURIDAD QUE TIENE LA UNIVERSIDAD CON RELACIÓN AL MANEJO DE INFORMACIÓN?

Esta pregunta cuenta con las siguientes opciones:

A. Si
B. No

Tabla 41. Conocimiento Políticas Seguridad por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	8	11	10	24	18	5	4
B	28	56	33	60	36	14	10

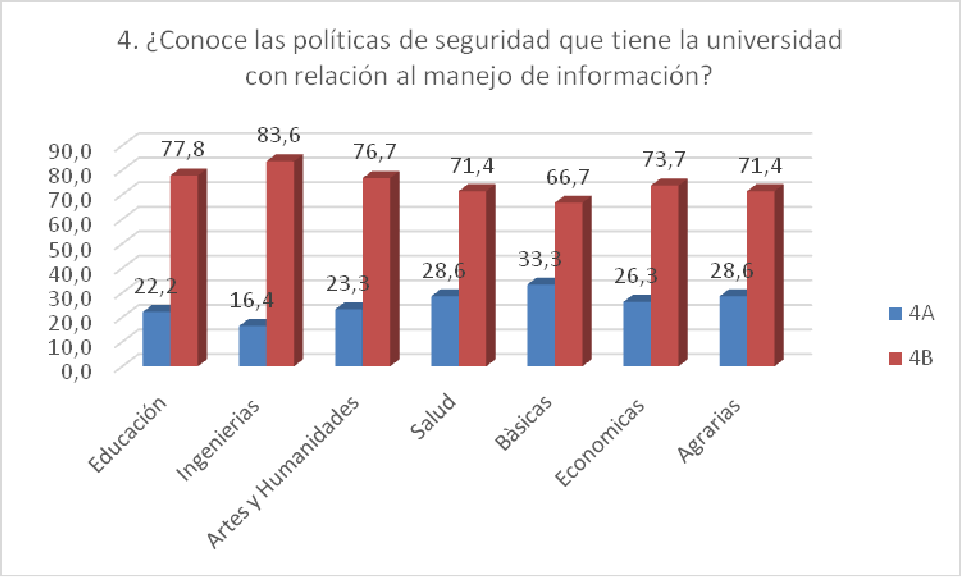

Figura 22. Porcentaje de Conocimiento de Políticas de Seguridad

B.1.6 PREGUNTA5: ¿DESDE QUÉ SITIO INGRESA CON MÁS FRECUENCIA AL CAMPUS TI?

Esta pregunta cuenta con las siguientes opciones:

A. Café internet
B. Celular personal
C. Portátil personal
D. Otro

Tabla 42. Lugar de Ingreso a Campus TI por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	1	2	5	5	1	0	0
B	7	3	0	8	1	0	0
C	24	56	35	66	50	19	12
D	4	6	3	5	2	0	2

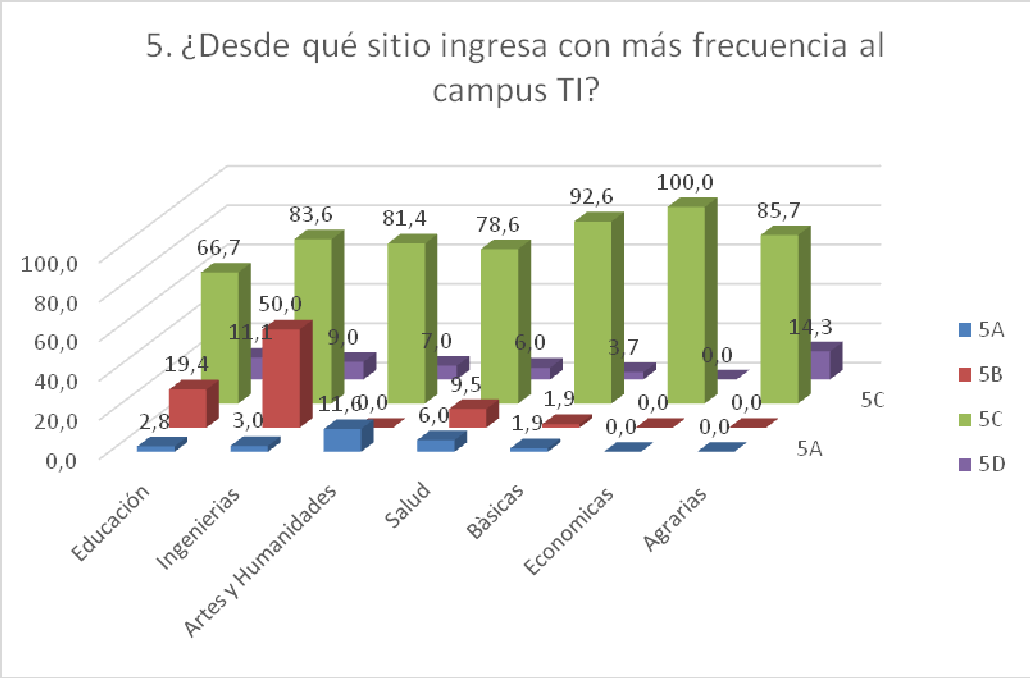

Figura 23. Porcentaje de Lugar de Ingreso a Campus TI

B.1.7 PREGUNTA 6: ¿CON QUE FRECUENCIA SE LE PRESENTAN PROBLEMAS PARA RECORDAR SU CONTRASEÑA DEL CAMPUS TI?

Esta pregunta cuenta con las siguientes opciones:

A. Cada vez que ingresa.
B. Después de una semana a un mes de no ingresar.
C. Después de dos meses
D. Nunca

Tabla 43. Problemas para Recordar Contraseña por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	1	4	0	0	3	0	0
B	4	8	0	10	4	15	0
C	14	20	18	37	21	4	8
D	17	35	25	37	26	0	6

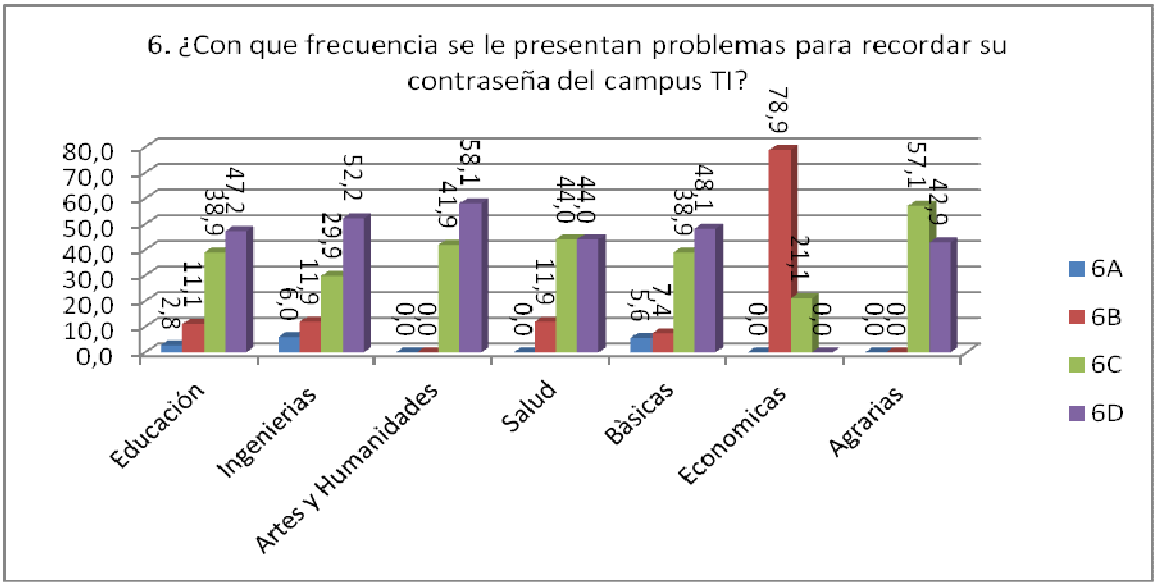

Figura 24. Porcentaje de Problemas para Recordar Contraseña

B.1.8 PREGUNTA 7: ¿EN QUÉ SITIO SUELE GUARDAR SU CONTRASEÑA DE ACCESO AL CAMPUS TI?

Esta pregunta cuenta con las siguientes opciones:

A. La escribe en un papel
B. La guarda en su correo electrónico
C. La guarda en el correo electrónico de un amigo
D. La memoriza
E. Usa un gestor de contraseñas.
F. Otra

Tabla 44. Sitio para Guardar Contraseña por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	0	8	3	5	3	0	0
B	5	0	0	5	1	4	2
C	0	2	0	3	0	0	0
D	29	57	35	64	48	15	11
E	0	0	0	0	2	0	0
F	2	0	5	7	0	0	1

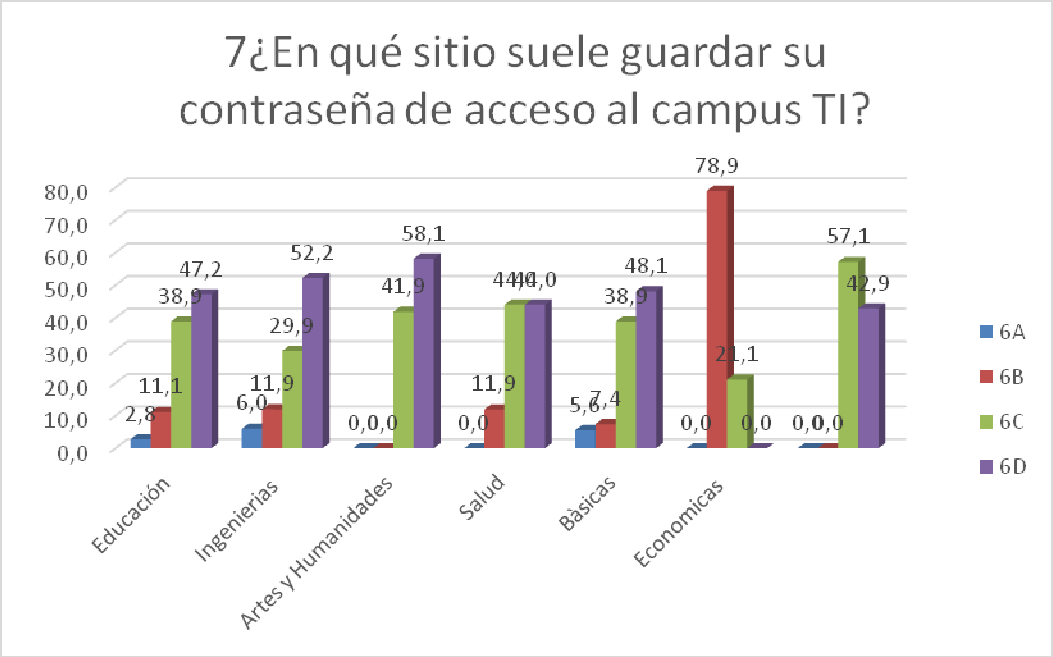

Figura 25. Porcentaje de Sitio para Guardar Contraseña

B.1.9 PREGUNTA 8: ¿CUÁNDO INGRESA AL PORTAL DEL CAMPUS: TOMA PRECAUCIONES PARA NO REVELAR SU CONTRASEÑA?

Esta pregunta cuenta con las siguientes opciones:

A. Si toma precauciones
B. No toma precauciones
C. Le da Igual
D. Otro cual

Tabla 45. Precauciones para No Revelar Contraseña por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	23	40	8	62	40	15	10
B	6	17	23	15	12	4	3
C	5	10	15	7	2	0	1
D	0	0	0	0	0	0	0
NR	2	0	5	0	0	0	0

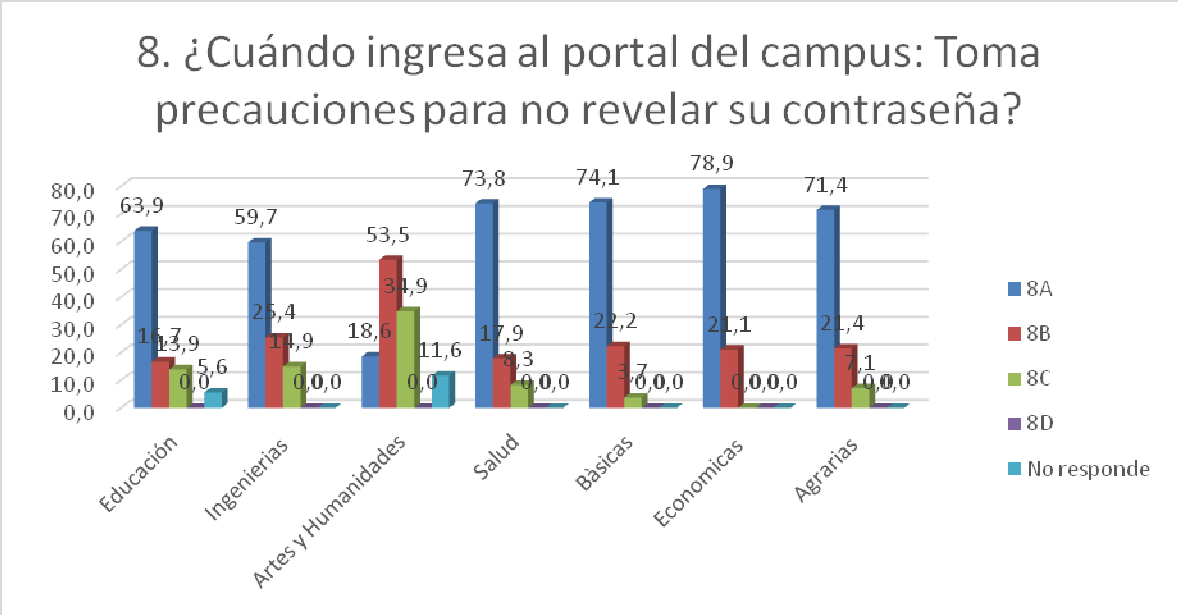

Figura 26 . Porcentaje de Precauciones para No Revelar Contraseña

B.1.10 PREGUNTA 9: ¿LAS NOTAS DE LOS ESTUDIANTES QUE DESCARGA DEL CAMPUS TI, DURANTE EL SEMESTRE, LAS ALMACENA EN?

Esta pregunta cuenta con las siguientes opciones:

A. USB
B. Papel
C. Portátil
D. Otro medio

Tabla 46. Sitio Almacenamiento Notas Estudiantes por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	9	11	9	8	7	4	4
B	1	4	15	15	3	15	1
C	19	43	5	59	38	10	9
D	5	9	20	2	6	0	0
NR	2	0	3	0	0	0	0

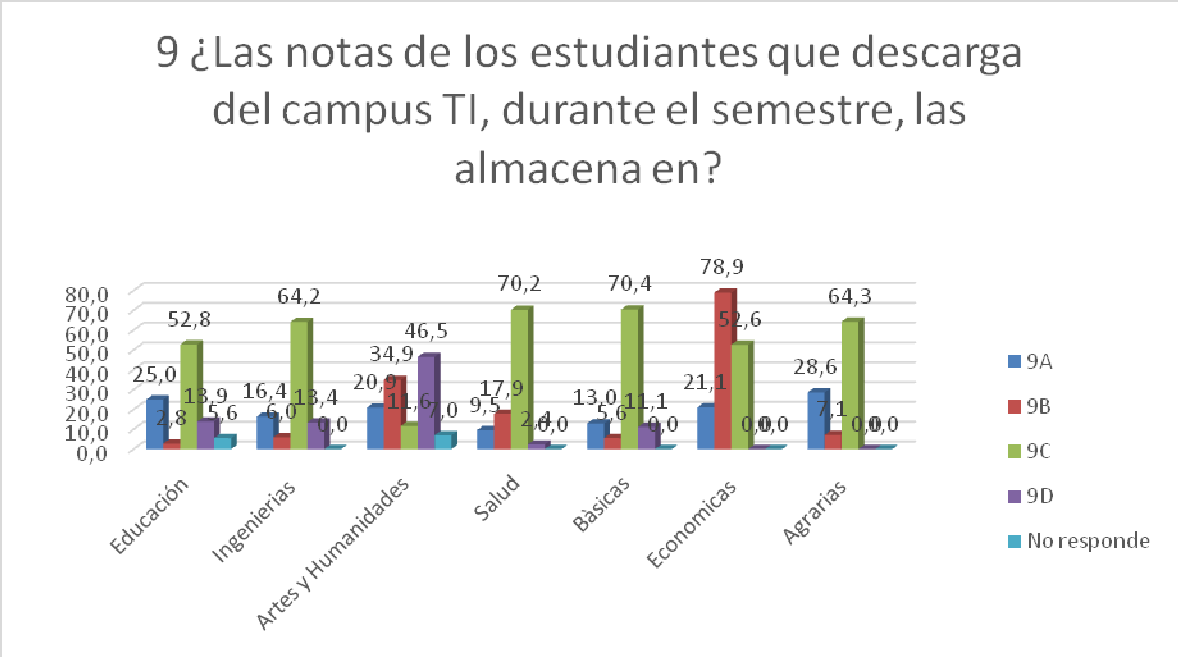

Figura 27 . Porcentaje Sitio de Almacenamiento Notas Estudiantes

B.1.11 PREGUNTA 10: ¿LAS NOTAS DE LOS ESTUDIANTES QUE DESCARGA DEL CAMPUS TI, DURANTE EL SEMESTRE Y ALMACENA EN MEDIOS DIGITALES LAS CIFRA?

Esta pregunta cuenta con las siguientes opciones:

A. Si
B. No

Tabla 47. Cifrado de Notas de Estudiantes por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	21	23	15	45	19	15	7
B	14	44	28	39	35	4	7
NR	1	0	0	0	0	0	0

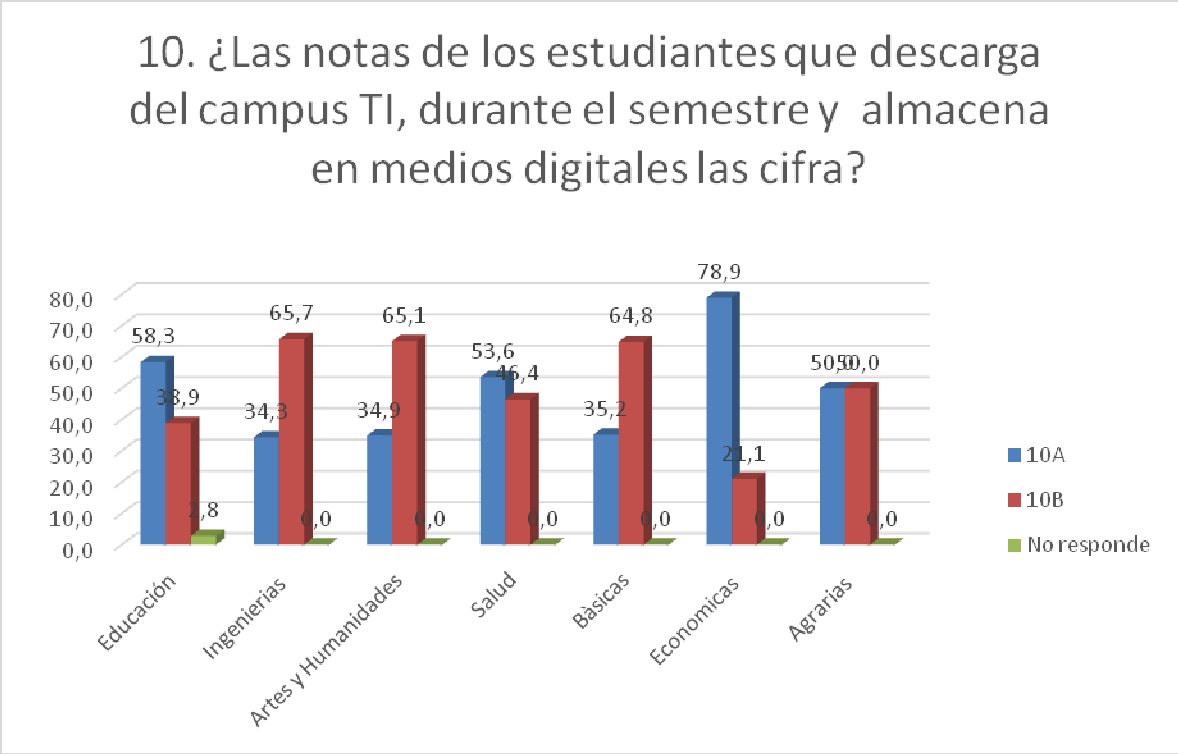

Figura 28 . Porcentaje de Cifrado de Notas de Estudiantes

B.1.12 PREGUNTA 11: AL MEDIO DONDE ALMACENA LAS NOTAS DE LOS ESTUDIANTES TIENE ACCESO

Esta pregunta cuenta con las siguientes opciones:

A. Solo usted
B. Otras personas

Tabla 48 . Personas con Acceso a Medio de Almacenamiento de Notas por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	34	61	11	77	50	19	14
B	1	6	40	7	4	0	0
NO GUARDA	1	0	3	0	0	0	0

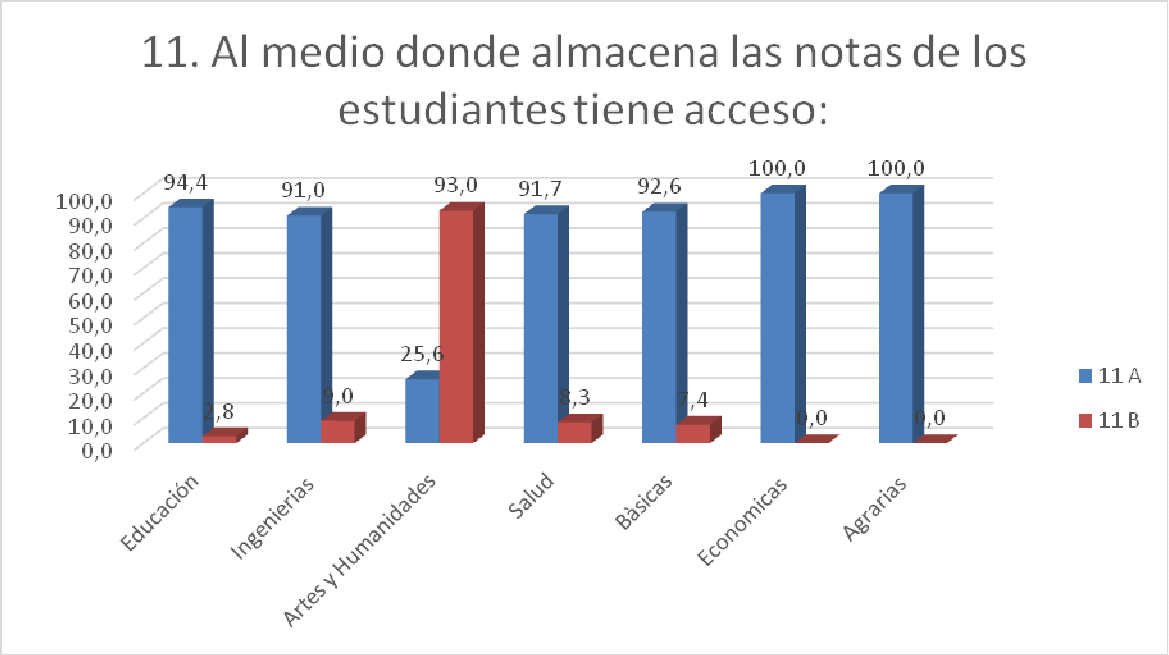

Figura 29. Porcentaje de Personas con Acceso a Medio de Almacenamiento de Notas

B.1.13 PREGUNTA 12: ¿DESPUÉS DE TERMINADO EL SEMESTRE QUE HACE CON LAS NOTAS Y LISTAS DE LOS ESTUDIANTES?

Esta pregunta cuenta con las siguientes opciones:

A. Las destruye.
B. Deja una copia de seguridad en su correo
C. Deja una copia de seguridad en la nube.
D. Deja una copia de seguridad en portátil.
E. Deja una copia de seguridad en memoria. USB o disco externo
F. Deja una copia impresa
G. Otro

Tabla 49. Copia de Notas Terminado Semestre por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	3	4	12	5	5	5	5
B	7	13	5	20	12	0	0
C	1	2	5	5	2	0	0
D	20	32	3	35	29	9	5
E	3	5	18	8	4	5	1
F	1	2	3	3	1	0	3
G	0	9	5	8	3	0	0

NO GUARDA	1	0	4	0	0	0	0

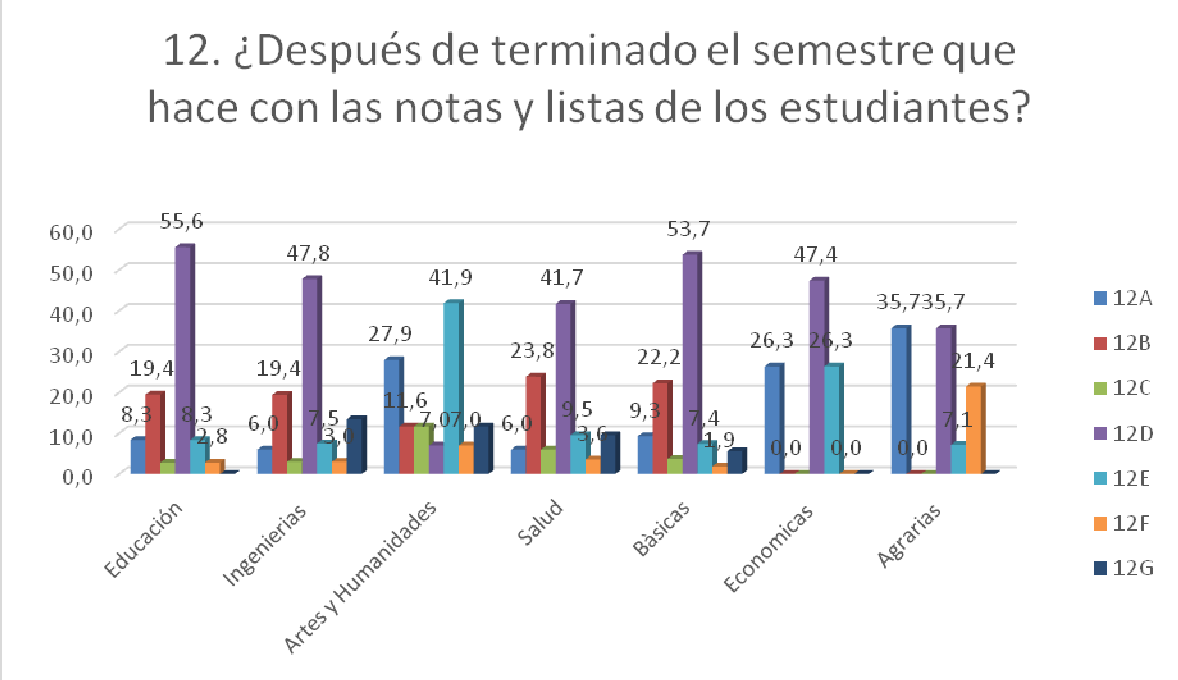

Figura 30. Porcentaje de Copia de Notas Terminado Semestre

B.2 ENCUESTAS A ESTUDIANTES

B.2.1 GÉNERO DE PARTICIPANTES

Tabla 50. Género de Participantes por Facultades

GÉNERO	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
Femenino	31	53	20	61	10	11	7
Masculino	18	91	18	49	7	12	18
Total	49	144	38	110	17	23	25

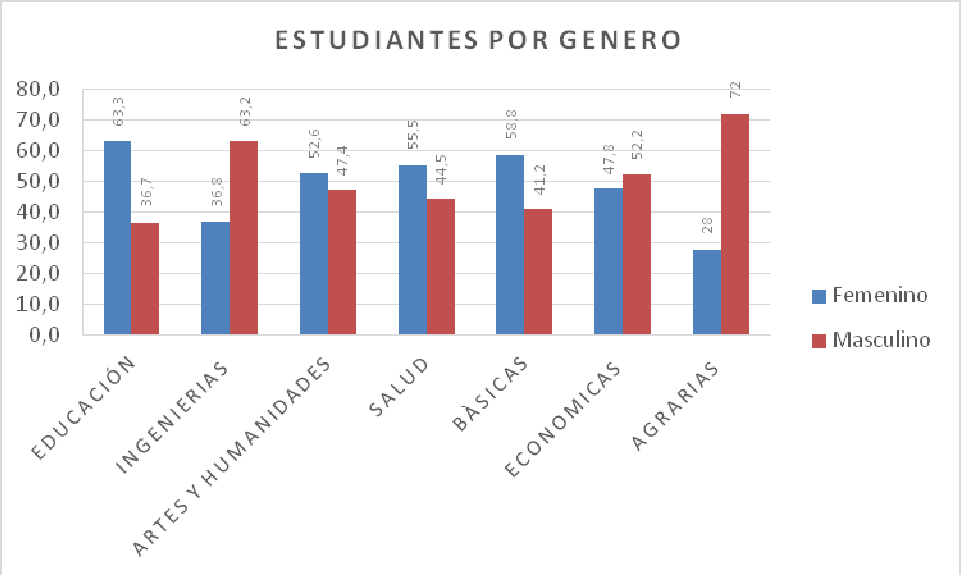

Figura 31. Porcentaje de Participantes por Género

B.2.2 PREGUNTA 1: ¿CUÁNTAS PERSONAS CONOCEN SU CONTRASEÑA DE INGRESO AL CAMPUS TI?

Esta pregunta cuenta con las siguientes opciones:

A. Solo usted
B. 2 personas
C. 3 personas o más

Tabla 51.Personas que Conocen Contraseña Campus TI por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	41	128	24	88	15	16	19
B	8	15	14	20	2	6	6
C	0	1	0	2	0	1	0

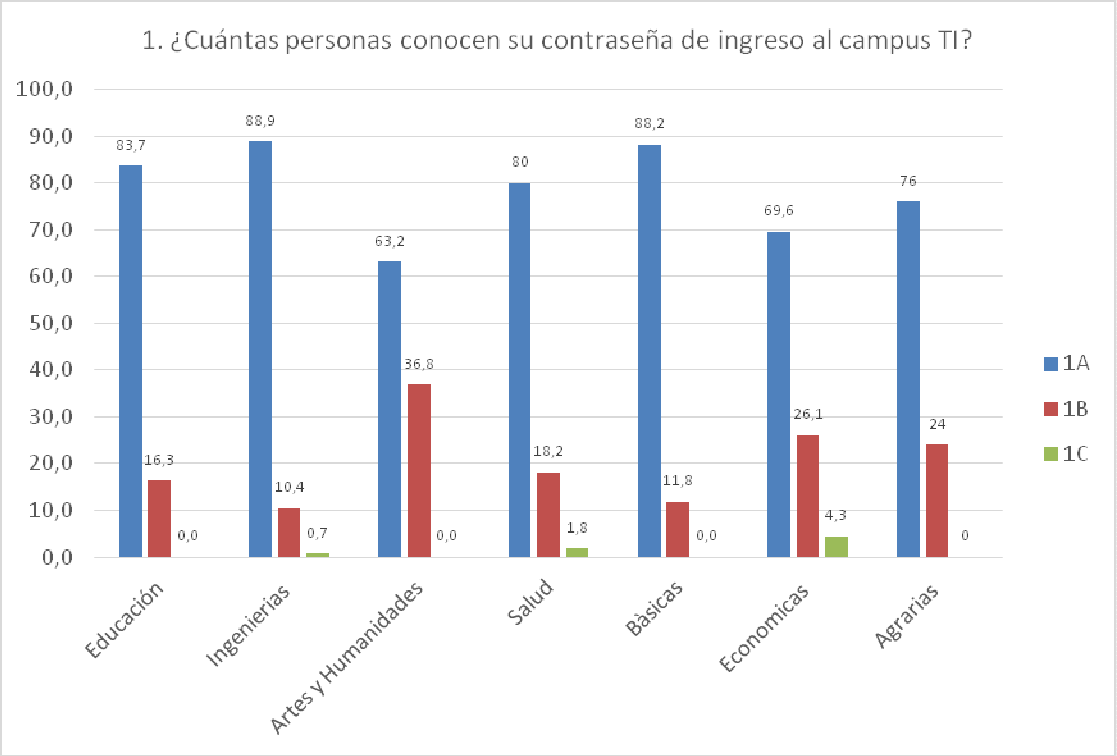

Figura 32. Porcentaje de Personas que Conocen Contraseña Campus TI

B.2.3 PREGUNTA 2: ¿LA LONGITUD DE SU CONTRASEÑA DE INGRESO AL CAMPUS TI?

Esta pregunta cuenta con las siguientes opciones:

A. 1 a 4 caracteres
B. 5 a 7 caracteres
C. 8 o más caracteres

Tabla 52. Longitud Contraseña Campus TI por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	2	2	4	3	0	0	1
B	23	98	24	57	12	12	19
C	24	44	10	50	5	11	5

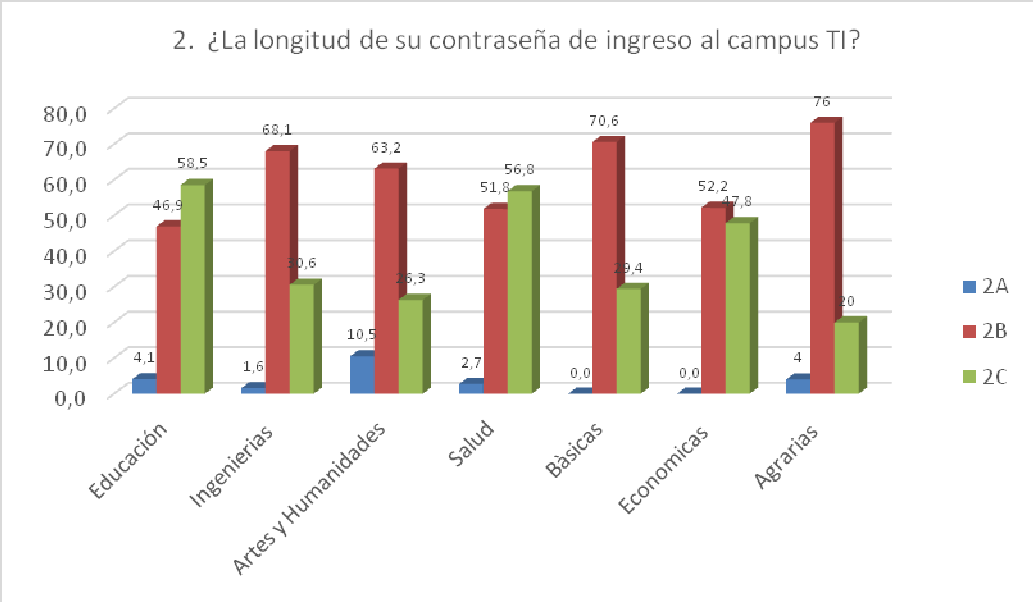

Figura 33. Porcentaje de Longitud de Contraseña Ingreso Campus TI

B.2.4 PREGUNTA 3: CUANDO ELIGE LA CONTRASEÑA DE INGRESO A SU CAMPUS TI

Esta pregunta cuenta con las siguientes opciones:

A. Prefiere una contraseña compleja y fácil de recordar.
B. Prefiere una contraseña compleja y difícil de recordar.
C. Prefiere una contraseña sencilla y fácil de recordar.
D. No le da importancia

Tabla 53. Complejidad Contraseña Campus TI por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	24	70	23	57	7	14	10
B	3	7	0	2	0	1	1
C	16	49	14	34	8	5	12
D	6	18	1	17	2	3	1

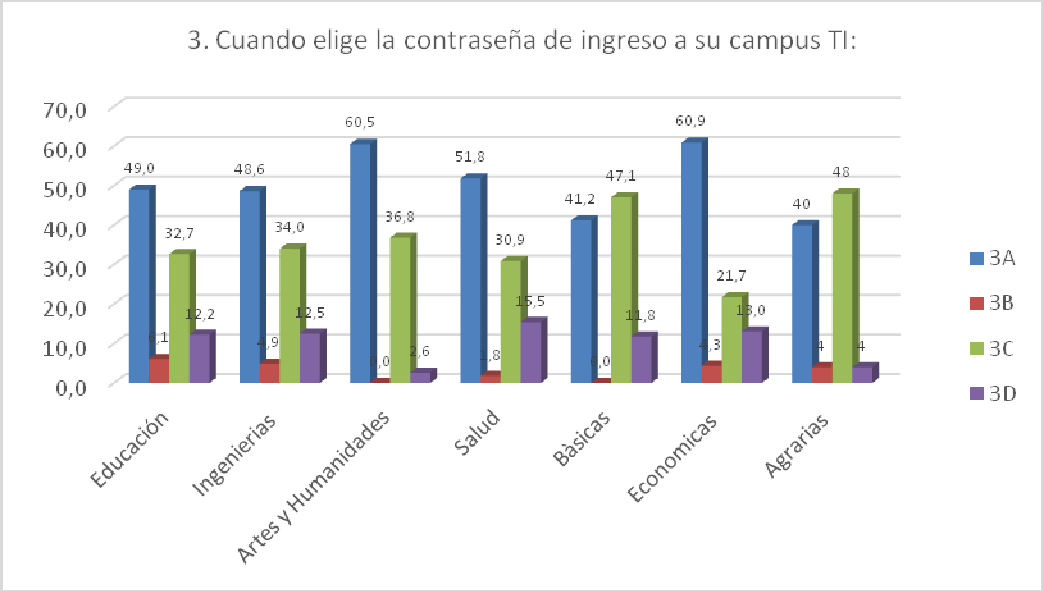

Figura 34. Porcentaje Complejidad Contraseña Campus TI

B.2.5 PREGUNTA 4: ¿CONOCE LAS POLÍTICAS DE SEGURIDAD QUE TIENE LA UNIVERSIDAD CON RELACIÓN AL MANEJO DE INFORMACIÓN?

Esta pregunta cuenta con las siguientes opciones:

A. Si
B. No

Tabla 54. Conocimiento Políticas Seguridad por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	3	3	5	15	2	1	0
B	46	141	33	95	15	22	25

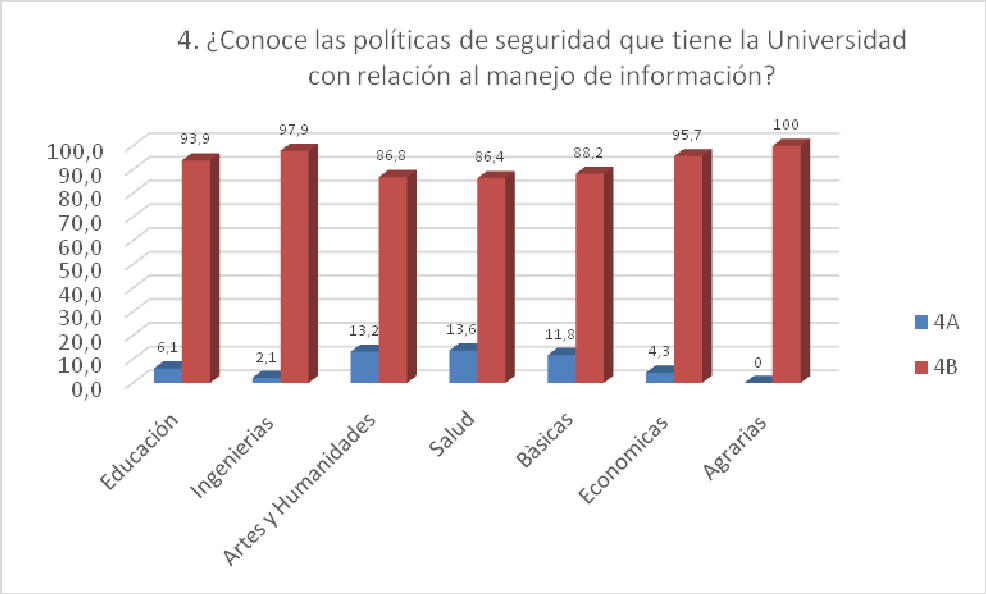

Figura 35. Porcentaje de Conocimiento de Políticas de Seguridad

B.2.6 PREGUNTA5: ¿DESDE QUÉ SITIO INGRESA CON MÁS FRECUENCIA AL CAMPUS TI?

Esta pregunta cuenta con las siguientes opciones:

A. Café internet
B. Celular personal
C. Portátil personal
D. Otro

Tabla 55. Lugar de Ingreso a Campus TI por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	2	1	3	5	1	0	1
B	14	60	11	34	4	8	5
C	32	83	24	71	12	15	18
D	1	0	0	0	0	0	1

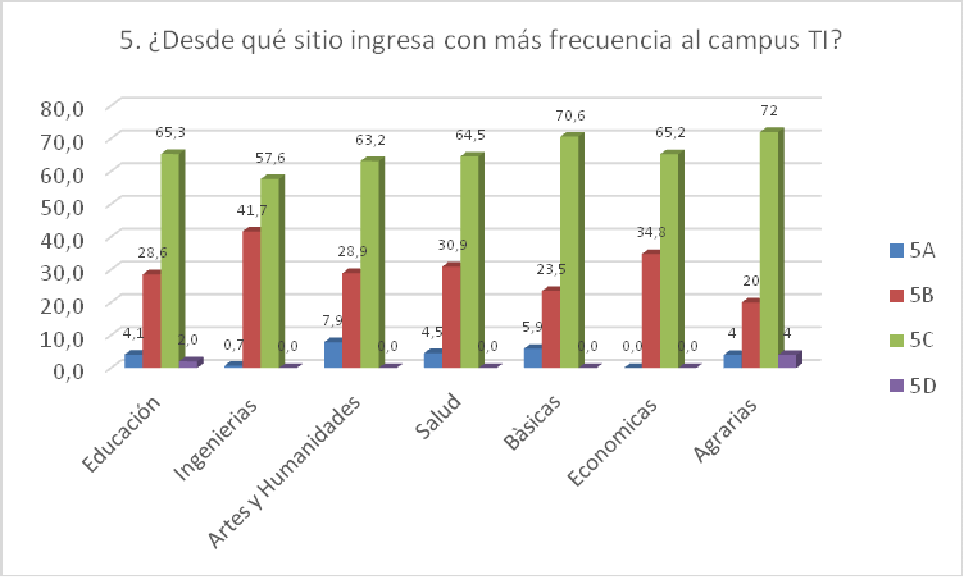

Figura 36. Porcentaje de Lugar de Ingreso a Campus TI

B.2.7 PREGUNTA 6: ¿CON QUE FRECUENCIA SE LE PRESENTAN PROBLEMAS PARA RECORDAR SU CONTRASEÑA DEL CAMPUS TI?

Esta pregunta cuenta con las siguientes opciones:

A. Cada vez que ingresa.
B. Después de una semana a un mes de no ingresar.
C. Después de dos meses
D. Nunca

Tabla 56. Problemas para Recordar Contraseña por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	0	0	0	2	0	0	1
B	11	10	4	11	2	1	1
C	8	27	7	19	5	3	4
D	30	107	27	78	10	19	19

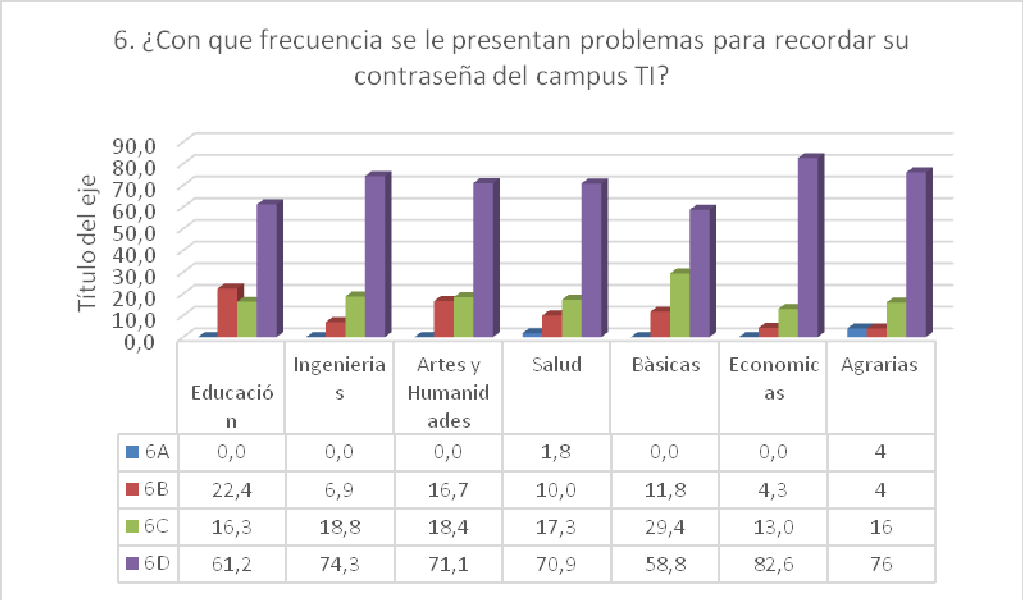

Figura 37. Porcentaje de Problemas para Recordar Contraseña

B.2.8 PREGUNTA 7: ¿EN QUÉ SITIO SUELE GUARDAR SU CONTRASEÑA DE ACCESO AL CAMPUS TI?

Esta pregunta cuenta con las siguientes opciones:

A. La escribe en un papel
B. La guarda en su correo electrónico
C. La guarda en el correo electrónico de un amigo
D. La memoriza
E. Usa un gestor de contraseñas.
F. Otra

Tabla 57. Sitio para Guardar Contraseña por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	2	0	2	1	0	0	2
B	2	0	2	2	0	1	1
C	0	0	0	0	0	0	20
D	40	140	30	94	17	21	0
E	0	1	2	7	0	0	0
F	5	3	2	6	0	1	2

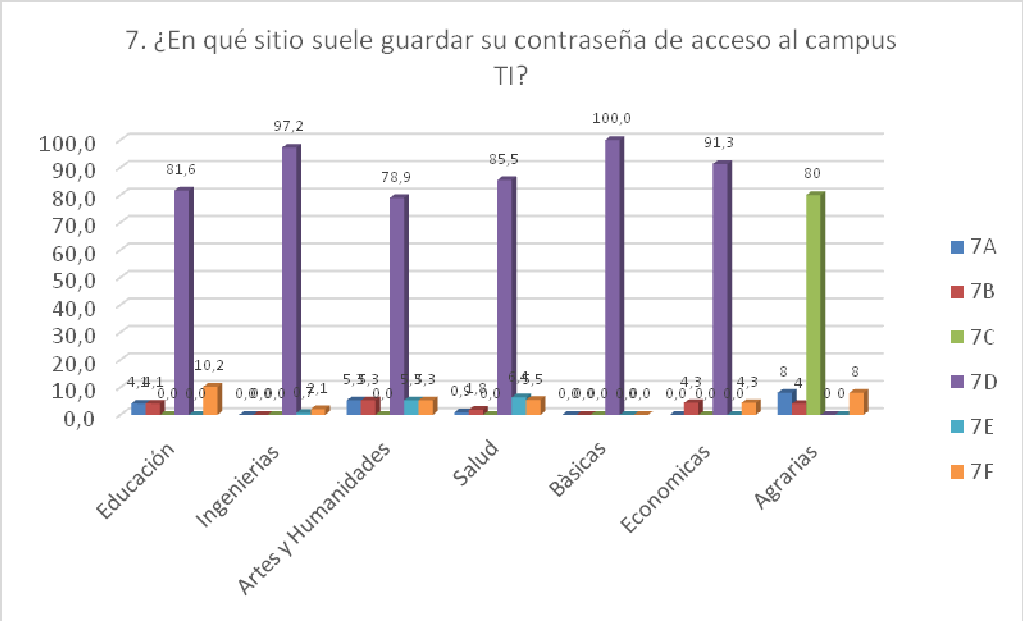

Figura 38. Porcentaje de Sitio para Guardar Contraseña

B.2.9 PREGUNTA 8: ¿CUÁNDO INGRESA AL PORTAL DEL CAMPUS: TOMA PRECAUCIONES PARA NO REVELAR SU CONTRASEÑA?

Esta pregunta cuenta con las siguientes opciones:

A. Si toma precauciones
B. No toma precauciones
C. Le da Igual
D. Otro

Tabla 58. Precauciones para No Revelar Contraseña por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	23	65	11	52	9	12	13
B	15	57	17	33	6	7	9
C	10	22	10	25	2	4	3
D	1	0	0	0	0	0	0

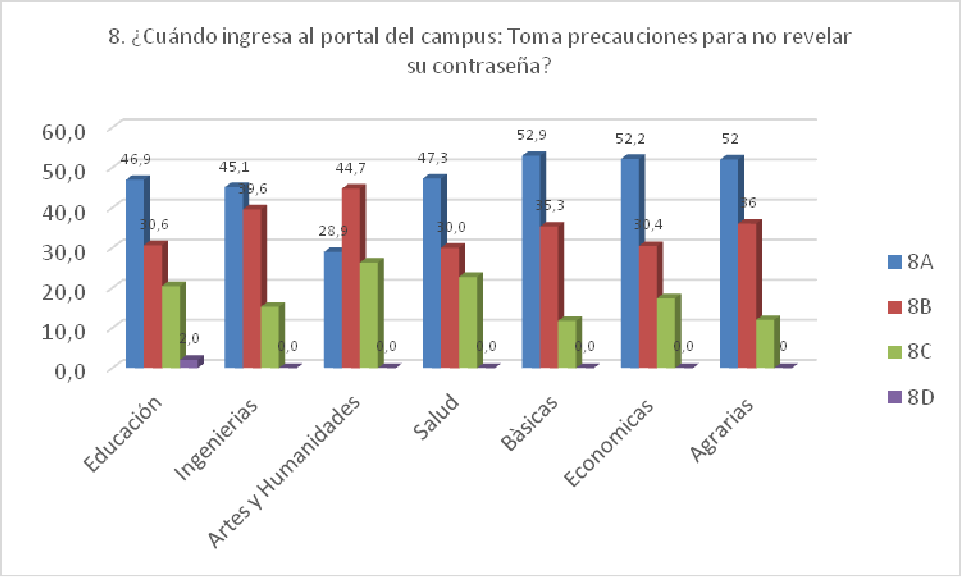

Figura 39 . Porcentaje de Precauciones para No Revelar Contraseña

B.2.10 PREGUNTA 9: ¿DÓNDE ALMACENA SUS NOTAS AL DESCARGARLAS DEL CAMPUS TI?

Esta pregunta cuenta con las siguientes opciones:

A. USB
B. Papel
C. Portátil
D. Otro medio

Tabla 59. Sitio Almacenamiento Notas por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	10	0	6	10	0	0	6
B	7	8	0	32	2	2	3
C	29	114	24	63	12	15	15
D	3	22	8	5	2	6	1

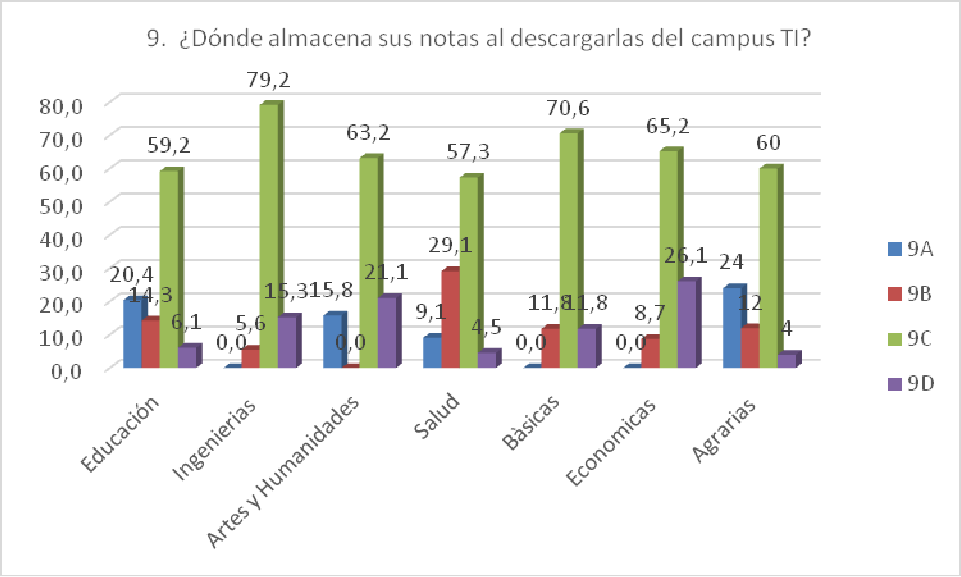

Figura 40 . Porcentaje Sitio de Almacenamiento Notas

B.2.11 PREGUNTA 10: ¿QUIÉN TIENE ACCESO A LA INFORMACIÓN QUE DESCARGA DEL CAMPUS?

Esta pregunta cuenta con las siguientes opciones:

A. Solo usted
B. Otras personas

Tabla 60. Acceso a Información Descargada por Facultades

OPCIÓN	EDUCACIÓN	INGENIERÍAS Y ARQUITECTURA	ARTES Y HUMANIDADES	SALUD	CIENCIAS BÁSICAS	CIENCIAS ECONÓMICAS	CIENCIAS AGRARIAS
A	44	127	32	97	14	20	20
B	5	17	6	13	3	3	5

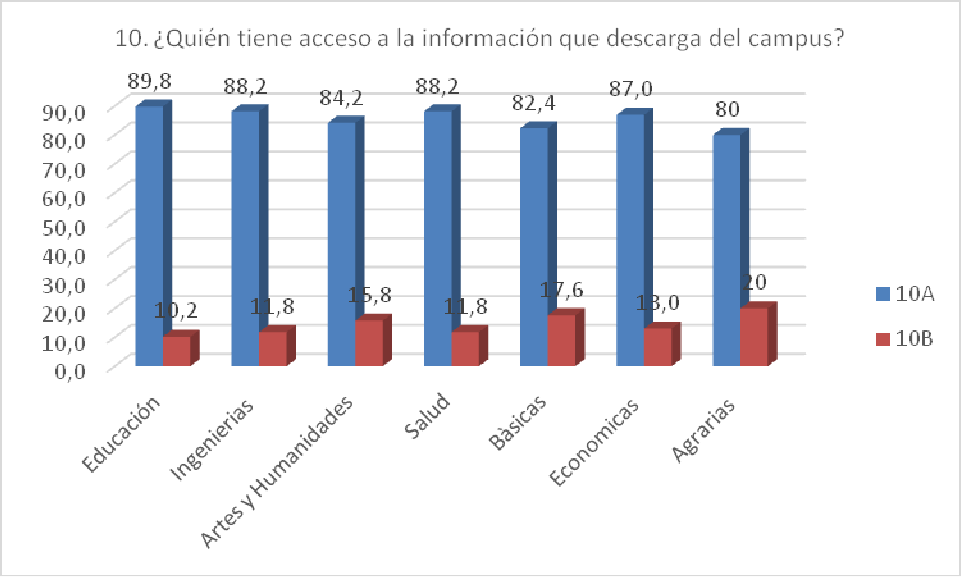

Figura 41 . Porcentaje de Acceso a Información Descargada

i