UNIVERSIDAD DE PAMPLONA
FACULTAD DE INGENIERÍAS Y ARQUITECTURA
DEPARTAMENTO DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, SISTEMAS Y TELECOMUNICACIONES

PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE INGENIERO EN TELECOMUNICACIONES

TÍTULO:
IMPLANTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE VILLANUEVA LA GUAJIRA, BASADO EN LA NORMA ISO/IEC 27001

Autor:
CARLOS ANDRES SARMIENTO COLLANTE

Director:
ING. ADRIANA VILLAMIZAR PEDRAZA

PAMPLONA-COLOMBIA

DICIEMBRE DE 2021

UNIVERSIDAD DE PAMPLONA
FACULTAD DE INGENIERÍAS Y ARQUITECTURA
DEPARTAMENTO DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, SISTEMAS Y TELECOMUNICACIONES

PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE INGENIERO EN TELECOMUNICACIONES

TÍTULO:

IMPLANTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDIA MUNICIPAL DE VILLANUEVA LA GUAJIRA, BASADO EN LA NORMA ISO/IEC 27001

Autor:
CARLOS ANDRES SARMIENTO COLLANTE

Director:
ING. ADRIANA VILLAMIZAR PEDRAZA

JURADO CALIFICADOR:
Ing. ADRIANA VILLAMIZAR PEDRAZA
Ing. EDWIN MAURICIO SEQUEDA ARENAS
Ing. JOSÉ DEL CARMEN PEÑA FERNANDEZ

PAMPLONA-COLOMBIA

DICIEMBRE DE 2021

UNIVERSIDAD DE PAMPLONA
FACULTAD DE INGENIERÍAS Y ARQUITECTURA
DEPARTAMENTO DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, SISTEMAS Y TELECOMUNICACIONES

PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES

TRABAJO PRESENTADO PARA OPTAR POR ÉL TITULO DE INGENIERO EN TELECOMUNICACIONES

TEMA:

IMPLANTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDIA MUNICIPAL DE VILLANUEVA LA GUAJIRA, BASADO EN LA NORMA ISO/IEC 27001

FECHA DE INICIO DEL TRABAJO: AGOSTO 2021

FECHA DE TERMINACION DEL TRABAJO:

NOMBRES Y FIRMAS DE AUTORIZACIÓN PARA LA SUSTENTACION:

_____
CARLOS ANDRES SARMIENTO COLLANTE
AUTOR

_____ _____
ING. ADRIANA VILLAMIZAR P. **ING. EDWIN SEQUEDA ARENAS**
DIRECTOR **DIRECTOR DEL PROGRAMA**

JURADO CALIFICADOR:

_____ _____
ING. ADRIANA VILLAMIZAR P. **ING. EDWIN SEQUEDA ARENAS**

_____
ING JOSÉ PEÑA FERNANDEZ.

PAMPLONA N. S. COLOMBIA
DICIEMBRE DE 2021

DEDICATORIA

Este trabajo es dedicado primeramente a Dios por darme cada día un motivo más para vivir y porque mi razón de superarme que es mi familia sigue aquí conmigo. A mis padres por dejarme volar tan lejos y hacer que mis sueños no fueran solo sueños, a mis hermanas por cuidar de ellos mientras no estuve yo. A esos compañeros de infancia del barrio Orozus que siempre han estado ahí desde que tengo memoria y están conmigo en todo momento, a mis hermanos Ramón Alberto, Eduin Jarli y Leo porque más allá de su amistad siempre han estado ahí con la buena vibra en las buenas, malas y peores. A mis mascotas que al llegar a casa me reciben de manera efusiva y son un motor más en mi vida.

A mis compas de Universidad: Sergio Andrés, Jhustin, Diego, Ana, Angie, Ledys, Eduin Alonso, Rubén, y a Sergio García "Superman", a quien conocí el primer día en clases de expresión gráfica y desde ese momento ratificamos que si hay hermanos que la vida misma se encarga de darnos. A Diego, Yeimi y Dieguito por hacerme sentir como en casa y ser mi segunda familia, ellos son mis padres y hermano de Pamplona.

Por Último, pero no menos importante, me lo dedico a mí, porque nunca dudé de mis capacidades y me he superado una vez tras otra a lo largo de este proceso. Ah, y muchísimas gracias a la persona de las velitas virtuales, esto también es de ella.

Y por allá bien lejos, más allá del cielo, se lo dedico a mi Tía Valentina Sanguino. Siempre estaré agradecido con ella por llevarme a conocer Pamplona, usted fue quien hizo que me enamorara de tan magnífico pueblo hasta el punto de no querer salir de allá hasta ser profesional. Lástima que no pueda ver este triunfo aquí en la tierra, pero sé que desde donde se encuentre siempre me cuida y yo la recordaré por siempre.

AGRADECIMIENTOS

Agradezco a todos los docentes que hicieron parte de mi proceso de formación, porque fueron quienes aportaron activamente sus conocimientos para hacer de mi un profesional ético, aplicado y capaz de enfrentar cualquier reto, de ustedes no solo me llevo sus enseñanzas sino también las anécdotas vividas a lo largo del camino. Gracias a la Ingeniera Adriana Villamizar, sé que no ha sido fácil este camino, pero gracias a sus aportes, a su amor por enseñar y apoyo constante, lo complicado de lograr esta meta se ha notado menos.

Gracias totales al Ingeniero Jacen por siempre estar presente durante mis prácticas y compartir sus conocimientos conmigo, a la Alcaldía Municipal de Villanueva La Guajira y a todos sus empleados, sentí como si llevara una vida trabajando junto a ellos.

CONTENIDO

1 INTRODUCCIÓN 1
1.1 Planteamiento del Problema 1
1.2 Justificación 3
1.3 Delimitación 4
1.3.1. Objetivo General 4
1.3.2 Objetivos Específicos 4

2 MARCO TEÓRICO 5
2.1 Sistema de gestión de seguridad de la información (SGSI) 5
2.2 International Organization for Standardization / International Electrotechnical Commission 27001 [ISO/IEC 27001] 6
2.3 Activos de información 7
2.4 Seguridad de la información 8
2.4.1 Privacidad: 8
2.4.2 Integridad: 8
2.4.3 Disponibilidad: 8
2.5 Amenaza 8
2.6 Riesgo 9
2.6.1. Riesgos estratégicos 9
2.6.2. Riesgos tácticos 9
2.6.3. Riesgos operacionales 9
2.7 Gestión del riesgo 9
2.8 Análisis del riesgo 10
2.9 Gestión de incidentes de seguridad de la información 10
2.10 Control 11

CAPÍTULO 3 12

3. MARCO LEGAL 12
3.1. Resolución 1443 de 2018 12
3.2. Resolución N°1519 de 2020 13
3.3. Ley 603 de 2000 14
3.4. Ley 1581 de 2012 14
3.5. Ley 1712 de 2014 14

CAPÍTULO 4 18

4. IDENTIFICACIÓN DE ACTIVOS Y FUENTES DE INFORMACIÓN 18
4.1. Generalidades de la entidad 18
4.1.1. Procesamiento e interpretación de datos 20
4.1.2. Análisis. 36
4.2. Inventario de activos de información 37

CAPÍTULO 5 42
5. PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 42
5.1. Modelo del Sistema de gestión de seguridad de la información 42
5.1.1. Modelo general del SGSI 43
5.2. Fases del modelo del SGSI 44
5.2.1. Fase 1: Diagnóstico inicial 45
5.2.2. Metodología de valoración de riesgo y estimación de niveles de riesgos 46
5.3. Evaluación de los controles de la norma ISO/IEC 27001 49
5.3.1. Fase 2: Estructuración del sistema de gestión 51
5.4. Fase 3: Planificación del sistema 52
5.4.1. Gestión de riesgos de seguridad de la información 52
5.4.2. Políticas y controles adicionales de seguridad de la información 53
CAPÍTULO 6 54
PLAN DE TRATAMIENTO DE RIESGOS Y METODOLOGÍA DE APLICACIÓN DE CONTROLES DEL SGSI 54
6.1 Plan de tratamiento de riesgos en la secretaría de gobierno municipal 54
6.1.1 Política de seguridad SGSI 54
6.1.2 Objetivo 54
6.1.3 Alcance 55
6.1.4 Desarrollo 55
6.1.5 Sanciones 61
6.2 Aplicación de controles Anexo A ISO/IEC 27001 61
CAPÍTULO 7 62
7 PLAN DE MEJORA CONTINUA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 62
7.1 Procedimiento de revisión de incidentes de seguridad de la información. 62
7.1.1 Interpretación del diagrama de flujo 64
7.2 Verificación de robustez del sistema de gestión 70
7.3 Suficiencia del SGSI 70
7.3.1 Niveles de escala de madurez 71
CONCLUSIONES 72
RECOMENDACIONES 75
BIBLIOGRAFÍA 76
ANEXOS 80
Ficha técnica perteneciente al Análisis. Del capítulo 4.1.1 80
Producto tipo: Gestión de incidentes de seguridad de la información. 84
Herramienta para determinar madurez del SGSI, perteneciente al capítulo 7.3.1 85

LISTA DE FIGURAS

Figura 2.1 Modelo PHVA del ciclo Deming 7
Figura 4.1 Mapa Ubicación Villanueva la Guajira 18
Figura 4.2 Organigrama Alcaldía municipal Villanueva.....19
Figura 4.3 Conocimiento sobre activo de información 21
Figura 4.4 Conocimiento de empleados relacionado al concepto de seguridad de la información 21
Figura 4.5 Tipo de computadores presentes en la secretaría de gobierno 22
Figura 4.6 Tipos de cuenta en los equipos institucionales de la sec. Gobierno 22
Figura 4.7 Porcentaje de uso de contraseñas para inicio de sesión 23
Figura 4.8 Empleados que comparten sus contraseñas. 23
Figura 4.9 Empleados que permiten el uso de su equipo por terceros 24
Figura 4.10 Organización de archivos digitales por carpetas 24
Figura 4.11 Seguridad en archivos digitales 25
Figura 4.12 Organización de documentos según su clasificación 25
Figura 4.13 Empleados que disponen de estantes 26
Figura 4.14 Estantes disponibles con cerraduras 26
Figura 4.15 Antivirus licenciados en equipos de la Sec. gobierno 27
Figura 4.16 Empleados que conocen qué es un virus informático 27
Figura 4.17 Conocimiento de empleados sobre cómo actuar al detectar un virus. 28
Figura 4.18 ¿Realizan copias de seguridad de la información? 28
Figura 4.19 Método implementado para copias de seguridad 28
Figura 4.20 Empleados que utilizan dispositivos extraíbles 29
Figura 4.21 Conocimientos sobre políticas de gestión de riesgos 29
Figura 4.22 Empleados que conocen las políticas de tratamiento de datos 30
Figura 4.23 Conocimiento sobre políticas de ahorro energético 30

Figura 4.24 Conocimiento de empleados relacionado a las políticas de seguridad de la información.....31
Figura 4.25 ¿Almacenan los empleados información personal en los equipos institucionales? 31
Figura 4.26 Existencia de plan de contingencia en las oficinas de la Sec. Gobierno 32
Figura 4.27 Estado de puertas y ventanas de la Sec. Gobierno.....32
Figura 4.28 Mantenimiento preventivo y correctivo a los equipos.....33
Figura 4.29 Frecuencia con la que los usuarios realizan mantenimiento.....33
Figura 4.30 Conocimiento de los empleados sobre delito informático 34
Figura 4.31 Conocimiento de los empleados sobre Phising 34
Figura 4.32 Recepción de correos no deseados a los empleados de la Sec. Gobierno. 35
Figura 4.33 Empleados que han recibido correos de suplantación de identidad ...35
Figura 4.34 Libertad para la instalación de software en equipos institucionales....36
Figura 5.1 Procedimiento SGSI 43
Figura 5.2 Fases para el desarrollo e implementación del SGSI 44
Figura 7.1 Diagrama de flujo: detección de incidentes 63
Figura 7.2 Etapa inicial el diagrama de flujo 64
Figura 7.3 Segunda etapa del diagrama de flujo 65
Figura 7.4 Tercera etapa diagrama de flujo 65
Figura 7.5 Cuarta etapa del diagrama de flujo.....66
Figura 7.6 Quinta etapa del diagrama de flujo 66
Figura 7.7 Sexta etapa diagrama de flujo 67
Figura 7.8 Etapa final del diagrama de flujo.....68

LISTA DE TABLAS

Tabla 4.1 Distribución funcionarios secretaría de gobierno y jurídica 20
Tabla 4.2 Encabezado de Inventario y clasificación de activos de información 37
Tabla 4.3 Inventario de activos de información según tipo de datos o información 38
Tabla 4.4 Inventario de activos de información según tipo de sistema o infraestructura 39
Tabla 4.5 Inventario de activos de información según personal por oficinas adscritas a la secretaría de gobierno municipal 40
Tabla 5.1 Tabla probabilidad con la que pueden ocurrir los riesgos 47
Tabla 5.2 Tabla de impacto en caso de incidentes de seguridad de los activos de información 48
Tabla 5.3 Mapa de evaluación, relación probabilidad/impacto 49
Tabla 5.4 Encabezado declaración de aplicabilidad SGSI.....50
Tabla 5.5 Criterios PHVA en la planificación del SGSI en la secretaría de gobierno municipal.....52
Tabla 7.1 Encabezado del Formato de control de incidentes de seguridad de la información 68

GLOSARIO

Amenaza: Posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema.

Ataque: es el intento de destruir, alterar robar o exponer un activo.

Autenticación: Es cuando se garantiza la veracidad de un documento.

Confidencialidad: Propiedad de que la información no está disponible o es entregada a personas que no están autorizadas.

Control: Medida por la cual se modifica el riesgo.

Disponibilidad: Propiedad de poder acceder y utilizar la información

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o una situación desconocida previamente que puede ser pertinente a la seguridad. (Organization, 2004)

Evento de seguridad de la información: Se refiere a algo que puede afectar los niveles de riesgo, sin afectar de forma necesaria al negocio o a la información.

Incidentes de seguridad de la información: es un evento que atenta directamente contra la disponibilidad, integridad y confidencialidad de la información.

Información documentada: Activos de información que pueden estar en cualquier formato y de distintas fuentes que han sido recolectados en una dependencia o en la entidad en general.

Monitoreo: Proceso constante que revisa el cumplimiento de las actividades programadas y verifica el cumplimiento de las mismas.

Objetivo: También conocido como meta(s), es un resultado deseado que una persona u organización planea y se compromete a lograr mediante el desarrollo de actividades específicas.

Políticas: Conjunto de normas implementadas dentro de una organización para el correcto funcionamiento de las actividades diarias.

Seguridad de la información (S.I): Es la preservación de la integridad, disponibilidad y confidencialidad de la información dentro de cualquier entidad o en el día a día.

Sistema de Gestión de Seguridad de la Información (SGSI): Sistema basado en enfoque hacia todos los riesgos globales de una organización con el objetivo de establecer, implementar, operar, revisar, mantener y mejorar la seguridad de la información. (ICONTEC, 2006)

Sistema de información: Se le atribuye este término a aquellos servicios, aplicaciones o activos de tecnología el cual está conformado por una serie de datos entrelazados o de común vínculo para lograr un objetivo específico.

Validación: Confirmación de cumplimiento de los requisitos para un uso específico a través de la entrega de evidencia objetiva.

Verificación: Confirmación de cumplimiento de los objetivos mediante pruebas presentadas.

Vulnerabilidad: Se define como vulnerabilidad a aquella debilidad de los sistemas que pueden ser aprovechados por delincuentes informáticos

Capítulo 1

INTRODUCCIÓN

1.1 Planteamiento del Problema.....1
1.2 Justificación.....3
1.3 Delimitación.....4

1.1 Planteamiento del Problema

El Ministerio de las Tecnologías de la información y las comunicaciones (MINTIC), y a través de la iniciativa de la subdirección de estándares y arquitectura de TI que en su programa de fortalecimiento de la gestión TI en el estado colombiano, entorno a la política de gobierno digital consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009, se diseñó una guía para la administración del riesgo y el diseño de controles en entidades públicas de la política de gobierno Digital, DECRETO 1008 DE 2018 : “El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia, Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.”(Decreto 1008 De 2018: Política De Gobierno Digital, 2018)

La alcaldía municipal de Villanueva- la Guajira es una entidad territorial nivel 6 ubicada en el sur del departamento de la Guajira donde laboran más de 50 personas, distribuidas en 15 oficinas, las cuales disponen de 18 equipos de

escritorio y más de 22 computadores personales para el desarrollo de sus actividades, por ser una entidad pública debe cumplir con los requerimientos que exige MINTIC relacionado a las políticas de seguridad digital, cuyo objetivo es garantizar la confidencialidad, integridad y disponibilidad de los activos que se administran al interior de la organización.

En la actualidad se han detectado problemáticas relacionadas a la vulnerabilidad que tiene la información que manejan los funcionarios de la entidad, siendo una amenaza al no realizar copias de seguridad, no existir un riguroso control de ingreso a las instalaciones, ni controles de acceso a los sistemas de cómputo , falta de política de eficiencia energética viéndose reflejado en la permanencia de computadores encendidos aún sin estarlos usando, exposición de hardware y archivos físicos (documentos, actas, contratos, hojas de vida) a posibles inundaciones y afectaciones ambientales que afectan la integridad de la información dado que no tiene infraestructura física adecuada que los resguarde; del total de 18 dependencias 5 carecen de cerraduras y ventanas en buen estado, situación que conllevan a la materialización de daños irreparables como la pérdida o robo de información física y digital, además, los funcionarios desconocen buenas prácticas referentes al manejo de seguridad de la información dado que no se han estipulado políticas de uso y no se han capacitado para actuar frente a las posibles amenazas que se puedan presentar, así mismo, la infraestructura tecnológica actual es deficiente para la demanda de servicios y administración que requiere la red. De lo anterior surge la siguiente pregunta:

¿Qué medidas y normas se pueden adoptar para disminuir los riesgos relacionados con la seguridad de la información en la alcaldía municipal de Villanueva La Guajira?

1.2 Justificación

El crecimiento desaforado de la internet y la sofisticación de la tecnología, conlleva a todos los usuarios a la obligación de mejorar las herramientas de seguridad de sus equipos activos y pasivos de red; la evolución del internet ha traído consigo la innovación de ataques cibernéticos en todo el mundo y Colombia no es la excepción; motivo por el cual que en el país surge la necesidad de realizar un modelo de gestión de tecnologías de la información para el estado, que incorpore aspectos de seguridad y privacidad de la información para así aumentar la capacidad de respuesta ante amenazas informáticas en todas las entidades públicas. El ministerio de tecnologías de la información y las comunicaciones MINTIC ha impulsado por medio de la iniciativa de gobierno digital el modelo de seguridad y privacidad de la información, alineándolo con el marco de referencia de arquitectura TI en las entidades territoriales a nivel nacional. En la alcaldía municipal de Villanueva la Guajira se hace necesario la creación de un Sistema de Gestión de seguridad de la información basado en la norma ISO/IEC 27001, que permita resolver y dar solución a las problemáticas detectadas entorno a la seguridad de los datos que posee la entidad, de esta manera, la entidad podrá disponer de los procedimientos, controles, protocolos diseñados a su medida para administrar y proteger los activos de la información, proporcionando la confidencialidad, disponibilidad e integridad de la información como lo exige la norma. El objetivo de este proyecto es asumir, controlar y proteger los activos mediante unos procedimientos sistémicos, documentados y conocidos por el personal, promoviendo a su vez la cultura apropiada de la seguridad para que los funcionarios fortalezcan los 3 pilares fundamentales, minimizando el riesgo y aumentando la capacidad de la organización para evitar o enfrentar amenazas asociadas al robo de información sensible sin importar el fin, dando así cumplimiento al enfoque planteado por el MINTIC.

1.3 Delimitación

1.3.1. Objetivo General

Implantar el Sistema de Gestión de seguridad de la información para la alcaldía municipal de Villanueva- La Guajira basado en la norma ISO/IEC 27001

1.3.2 Objetivos Específicos

- Identificar los activos y las fuentes de información que se usan actualmente en la alcaldía de Villanueva la Guajira.
- Planificar el sistema de gestión de seguridad de la información adaptando el ciclo Deming de acuerdo a la normativa ISO/IEC 27001.
- Implementar el plan de tratamiento de riesgos, políticas, controles, procesos y procedimientos del SGSI.
- Evaluar el sistema de gestión de seguridad de la información para generar el plan de mejora continua.

Capítulo 2

MARCO TEÓRICO

2.1 Sistema de gestión de seguridad de la información (SGSI) 5
2.2 International Organization for Standardization / International Electrotechnical Commission 27001 [ISO/IEC 27001] 6
2.3 Activos de información 7
2.4 Seguridad de la información 8
2.5 Amenaza 8
2.6 Riesgo 9
2.7 Gestión del riesgo 9
2.8 Análisis del riesgo 10
2.9 Gestión de incidentes de seguridad de la información 10
2.10 Control 11

2.1 Sistema de gestión de seguridad de la información (SGSI)

Consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales. Está reglamentado en la norma ISO/IEC 27001. (Javier Ruiz Spohr, 2005)

2.2 International Organization for Standardization / International Electrotechnical Commission 27001 [ISO/IEC 27001]

Es la norma principal, contiene los requisitos del SGSI. Dentro de su contenido está el anexo A, el cual enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo del SGSI. Este estándar internacional en Colombia está reglamentado por el Instituto Colombiano de Normas Técnicas y Certificación **(ICONTEC)** y recibe el nombre de NTC-ISO/IEC 27001, promoviendo la adopción de un enfoque basado en procesos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de la seguridad de la información en una organización (ICONTEC, 2006). La aplicación de un sistema de procesos dentro de la organización junto con la identificación, las interacciones y su gestión puede denominarse enfoque de procesos.

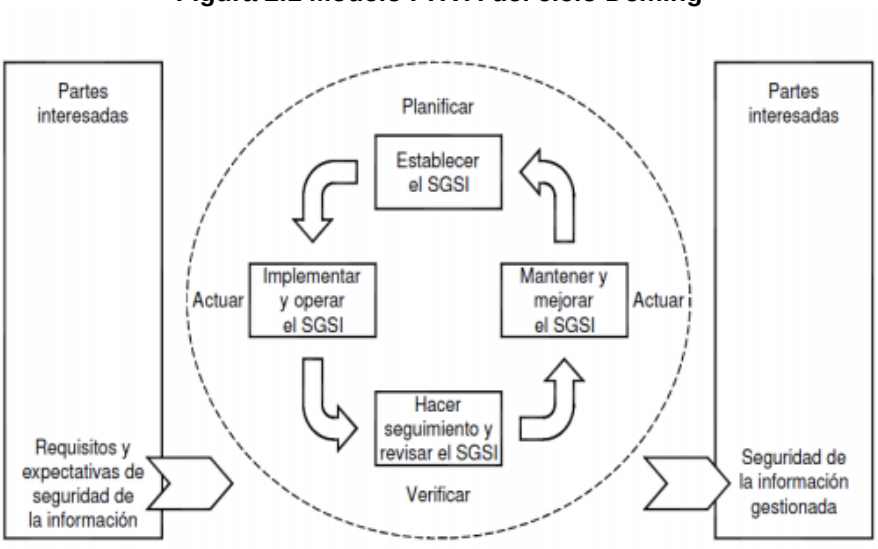
Un enfoque de procesos para la seguridad de la información enfatiza la importancia de:

a) Comprender los requisitos de seguridad de la información y la necesidad de establecer políticas y objetivos para la seguridad de la información.
b) Implementar y operar controles para gestionar los riesgos de seguridad de la información en una organización
c) Monitorear y revisar el desempeño y la efectividad de un SGSI y mejora continua basada en la medición objetiva. (Organization International Standard, 2018)

En la Figura 2.1 se observa que el estándar adopta el modelo Deming mejor conocido como “Plan-Do-Check-Act” (PDCA) o “Planear-Hacer-Verificar-Actuar”

(PHVA) en español, el cual es aplicado para estructurar todos los procesos del SGSI.

Figura 2.1 Modelo PHVA del ciclo Deming



Fuente (ICONTEC, 2006)

2.3 Activos de información

Se refiere a elementos de hardware y software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo (Consejo Nacional de política económica y social CONPES, 2016). Los activos de información dan soporte a las entidades relacionado a todos los procesos que se ejecutan dentro de ella, y comprende desde la identificación de cada elemento, el uso adecuado y en caso de algún infortunio, su recuperación; vale aclarar que se debe tener un cuidado riguroso con ellos debido a que siempre serán elementos vulnerables dentro de las empresas.

2.4 Seguridad de la información

Son todas las políticas de uso y medidas que afectan al tratamiento de los datos que se usan en una organización, es decir que son aquellas medidas preventivas y reactivas que permiten proteger la información. La seguridad de la información es un factor fundamental para que una entidad pueda llevar a cabo sus operaciones sin asumir muchos riesgos, debido a que los activos de información son una pieza fundamental para lograr cada uno de los objetivos de las organizaciones (TECON, 2018). La seguridad se basa en 3 pilares fundamentales: **Privacidad, integridad y disponibilidad.**

2.4.1 Privacidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (Javier Ruiz Spohr, 2005)

2.4.2 Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. (Javier Ruiz Spohr, 2005)

2.4.3 Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (Javier Ruiz Spohr, 2005)

Para poder coordinar las actividades de protección para la seguridad de la información cada organización debe establecer sus propias políticas y objetivos, y para poder lograrlos de manera eficaz se requiere en definitiva de un sistema de gestión de la seguridad de la información (o por sus siglas, SGSI)

2.5 Amenaza

Una amenaza es una causa potencial de un incidente no deseado, que puede provocar daños a un sistema atentando por ende a la seguridad de una organización (Organization International Standard, 2018). Toda amenaza surge gracias a la

aparición de vulnerabilidades en el sistema, es decir, que se define como una acción desencadenada al detectar una debilidad en un sistema de información que puede ser aprovechada por personas internas o externas a la organización con el objetivo de violar la seguridad y realizar daños, robos o secuestro de la información, lo cual resulta perjudicial para las organizaciones (Instituto nacional de ciberseguridad , 2017).

2.6 Riesgo

Se denomina riesgo a cualquier evento que en caso de ocurrir amenaza los objetivos de la organización (Instituto nacional de ciberseguridad , 2017). Existen 3 tipos de riesgos que son los riesgos estratégicos, tácticos y operacionales

2.6.1. Riesgos estratégicos

Este tipo de riesgo está orientado a los riesgos derivados de decisiones estratégicas que han sido tomadas en la organización o que lo serán a futuro.

2.6.2. Riesgos tácticos

Los riesgos tácticos son los asociados a los sistemas encargados de vigilar todo lo relacionado a los sistemas de identificación, control y monitoreo de posibles riesgos que pueden atentar contra la información de manera indirecta.

2.6.3. Riesgos operacionales

Los riesgos operacionales son los que están relacionados a los activos que pueden afectar los objetivos de una empresa, estos pueden ser los presupuestos, cronogramas, tecnologías, historial de finanzas, entre otros.

2.7 Gestión del riesgo

Es el proceso de identificar, comprender, evaluar y mitigar los riesgos y el impacto en la información, los sistemas de información y las organizaciones que

dependen de la información para sus operaciones. Además de identificar los riesgos y las medidas de mitigación de los mismos, un método y proceso de gestión del riesgo ayudará a:

- Identificar los activos críticos de información. Un programa de gestión de riesgos puede ampliarse para identificar también a personas críticas, procesos de negocio y tecnología.
- Comprender por qué los activos críticos escogidos son necesarios para las operaciones, la realización de la misión y la continuidad de las operaciones. (Sullivan, 2016)

2.8 Análisis del riesgo

Es el proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo (Organization International Standard, 2018). Para poder analizar y posteriormente identificar el potencial daño o pérdida se pueden responder las siguientes cuatro preguntas:

- ¿Cuál es la amenaza?
- ¿Cuál es el impacto?
- ¿Con qué frecuencia sucede?
- ¿Cuál es el grado de confianza, respeto a las respuestas de las tres primeras preguntas?

2.9 Gestión de incidentes de seguridad de la información

Son procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. La gestión de incidentes de seguridad de la información está compuesta por etapas, iniciando con la preparación ante un incidente de seguridad, seguido de las etapas de detección,

contención, erradicación, recuperación del incidente de seguridad de la información y finalizando con las lecciones aprendidas (MinCiencias, 2021).

2.10 Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

Capítulo 3

MARCO LEGAL

RESOLUCIÓN 1443 DE 2018....12
RESOLUCIÓN N°1519 DE 2020....13
LEY 603 DE 2000....14
LEY 1581 DE 2012....14
LEY 1712 DE 2014....14

3.1. Resolución 1443 de 2018

En esta resolución se conforma y establecen funciones de la dirección de gobierno digital; en relación a la conformación se enuncia en el decreto que el viceministro de tecnologías y sistemas de la información se transformó en el viceministro de economía digital, y las direcciones de estándares y arquitectura de TI, así como la de gobierno en línea pasan a ser subdirecciones adscritas a la nueva dirección.

Respecto a las funciones de la nueva dirección se establecieron las siguientes funciones:

- Formulación de políticas, lineamientos, estrategias y prácticas de gobierno en línea que soporten las gestiones del estado en orden al ejercicio de sus funciones de manera correcta y efectiva
- Liderar, articular e implementar con las entidades territoriales, las políticas y programas de ciudades inteligentes.

Por otra parte, el comité de sello de excelencia de gobierno digital conformado por:

- Viceministro de transformación digital, quien tendrá el cargo de presidente.
- Director de gobierno digital o quien haga sus veces.
- Subdirector de estándares y arquitectura de tecnologías de la información.
- Subdirector de fortalecimiento de capacidades públicas digitales.
- Coordinador del grupo interno de trabajo de servicios ciudadanos digitales. (MINTIC, 2018)

3.2. Resolución N°1519 de 2020

Conforme al principio de “Masificación del gobierno en línea” hoy llamado gobierno digital, consagrado en el numeral 3 del artículo 4 de la Ley 1341 de 2009 (Congreso de Colombia, 2009), se definen requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital y abiertos. En la ley 1341 se resalta promover el uso y apropiación de las TICs entre ciudadanos, empresas, el gobierno y demás instancias nacionales como parte del desarrollo social, económico y político de la nación.

En el artículo 18 Ley 1341 de 2009 también se establece que Mintic es responsable de diseñar, adoptar y promover políticas, planes y proyectos en el sector TIC para facilitar y optimizar la gestión de los organismos nacionales, prestando un mejor servicio a los usuarios.

En el anexo 3, apartado 3.2 de la resolución 1519 de 2020 se establecen condiciones de seguridad digital las cuales deberán ser adoptadas por los sujetos obligados para garantizar la seguridad digital y reducir los riesgos asociados a incidentes cibernéticos o filtración de datos sensibles. Además, exige la adopción de políticas de manera autónoma para la implementación de un **sistema de gestión de seguridad digital y de seguridad de la información**, recomendando los

estándares de la familia ISO 27000 y el modelo de seguridad y privacidad de la información (**MSPI**) elaborado por la dirección de gobierno digital del ministerio de las TIC (MINTIC, 2020).

3.3. Ley 603 de 2000

Esta ley permite la protección de la propiedad industrial y los derechos de autor. Por propiedad industrial se entiende la protección otorgada a las marcas, patentes o diseños industriales; y por derecho de autor se entienden obras creadas por personas individuales o talento humano que se materializan de manera original, ejemplos de estos son los derechos de autor de pinturas, obras literarias, software, películas, etc. (Congreso de la república, 2020)

3.4. Ley 1581 de 2012

La ley 1581 de 2012 o ley de protección de datos personales, tiene como objetivo desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, definiendo su ámbito de aplicación, principios, las categorías especiales de datos, el procedimiento para el tratamiento de los datos, los derechos que rigen los titulares de la información, las situaciones necesarias de autorización por parte del titular, el proceso para la corrección de información cuando sea necesario, deberes de responsables y encargados del tratamiento y los demás derechos, libertades y garantías constitucionales, así como el derecho a la información consagrado en el artículo 20 de la constitución política. El tratamiento de datos al que se refiere la ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen (Función pública, 2012).

3.5. Ley 1712 de 2014

En la presente ley se crea la ley de transparencia y del derecho de acceso a la información pública Nacional, los procedimientos para el ejercicio y garantía del

derecho y las excepciones a la publicidad de la información (Función Pública, 2014). Esta norma entró en vigencia en el año 2014 y además de regular el derecho de acceso a la información también estableció en el artículo 3 unos principios de la transparencia y acceso a la información pública enunciados a continuación:

- **Principio de transparencia**: En este principio toda la información que está en poder de los sujetos obligados definidos en la ley se presume pública, por lo cual se proporcionará el acceso a la misma excluyendo lo que esté sujeto a las excepciones legales bajo el cumplimiento de los requisitos de la ley.
- **Principio de buena fe**: La persona o funcionario al cumplir con obligaciones del derecho de acceso a la información pública, lo hará de manera honesta y leal.
- **Principio de facilitación:** Se facilitará el derecho de acceso a la información, siendo excluidas aquellos requisitos que impidan hacerlo.
- **Principio de no discriminación:** Se entregará la información a todas las personas que lo soliciten, independientemente de su raza, color, credo, orientación sexual, y sin exigir causas que motivan la solicitud.
- **Principio de gratuidad:** La información pública es gratuita y no se cobrará por su reproducción.
- **Principio de celeridad:** El trámite para a entrega de la información será ágil, principio fundamental en el cumplimiento de tareas a cargo de las entidades y los servidores públicos.
- **Principio de eficacia:** En búsqueda de la efectividad de los derechos colectivos e individuales de las entidades públicas, se busca lograr un número de resultados relacionados con las responsabilidades delegadas a cada organismo del estado.
- **Principio de la calidad de la información:** Toda la información producida, gestionada y difundida por el sujeto obligado, deberá ser oportuna, objetiva, veraz, completa reutilizable, procesable y debe estar disponible en formatos

accesibles para los interesados, pero aplicando siempre los procedimientos de gestión documental de la entidad.

- **Principio de la responsabilidad en el uso de la información:** Cualquier persona que haga uso de la información proporcionada por los sujetos obligados, lo hará atendiendo a la misma
- **Principio de la divulgación proactiva de la información:** El derecho a la información no está basado únicamente en la obligación de dar respuestas a peticiones, sino también en el deber de todos los sujetos obligado de incentivar y generar una cultura transparente, que implica la publicación y difusión de documentos que contengan la actividad institucional de interés público de manera rutinaria, proactiva, actualizada, accesible y comprensible, atendiendo a políticas y normas establecidas por el personal de recursos humanos, físicos y financieros.

En el artículo 5 de la presente ley también se define el significado de **sujetos obligados** haciendo referencia a:

- Entidades públicas de orden nacional, departamental, municipal y distrital
- Órganos, organismos y entidades estatales autónomas y de control
- Personas naturales y jurídicas, públicas o privadas que presten servicios públicos relacionados con la prestación del servicio público.
- Personas naturales y jurídicas que desempeñan función pública o de autoridad pública que esté relacionada con la prestación del servicio público.
- Empresas del estado o sociedades donde Éste tenga participación.
- Partidos, movimientos políticos y grupos significativos de ciudadanos
- Entidades administradoras de fondos o recursos de naturaleza u origen público. (SUIN, 2014)

En el **decreto 103 de 2015**, se realizaron unas reglamentaciones a la presente ley en los temas relacionados con la gestión de la información pública en

cuanto a su adecuada publicación y divulgación, la recepción y respuesta a solicitudes de esta, su adecuada clasificación y reserva, la elaboración de los instrumentos de gestión de información y el seguimiento. (SUIN, 2015).

Capítulo 4

IDENTIFICACIÓN DE ACTIVOS Y FUENTES DE INFORMACIÓN

4.1. Generalidades de la entidad.....18
4.2. Inventario de activos de información 37

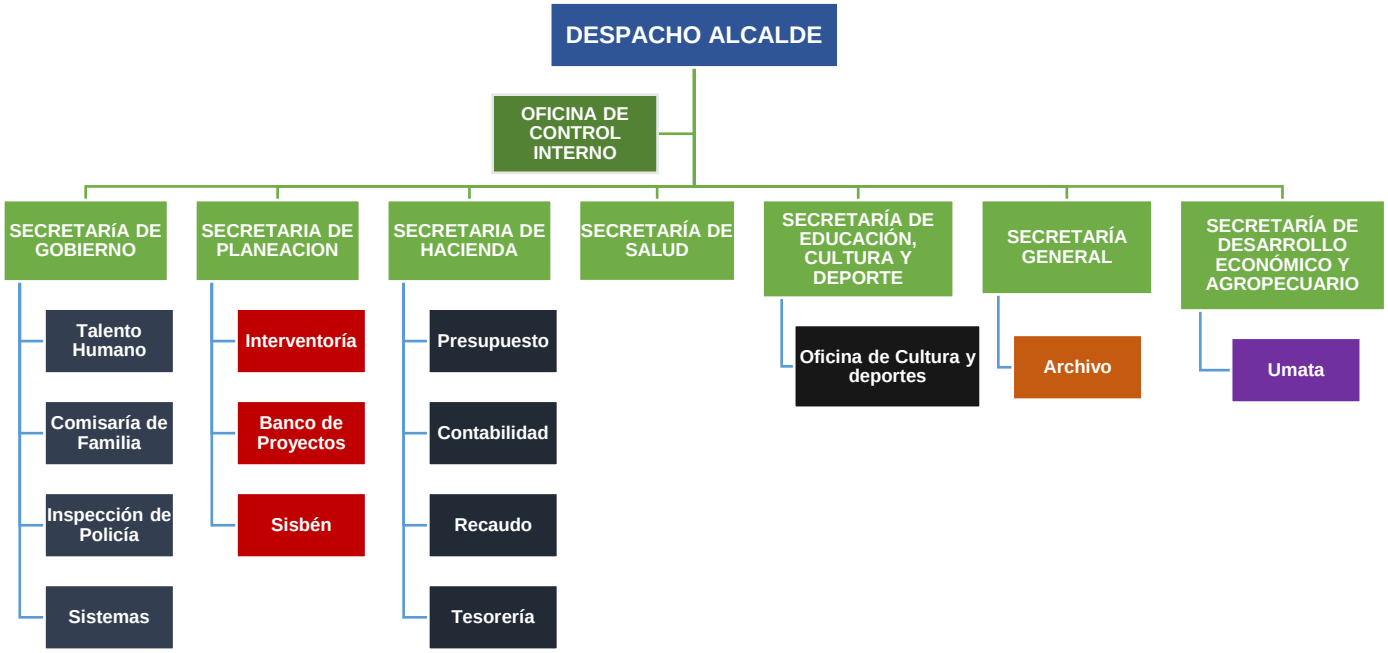
4.1. Generalidades de la entidad

El municipio de Villanueva La Guajira se encuentra ubicado al sur del departamento de la Guajira en la Costa Norte Colombiana, en la Figura 4.1 se observa su ubicación dentro del departamento; en cuanto a sus límites, la población limita al norte del municipio de El Molino, al sur con el municipio de Urumita, al Occidente con el departamento del cesar y al Oriente con la república Bolivariana de Venezuela.

Figura 4.1 Mapa Ubicación Villanueva la Guajira

La Alcaldía de Villanueva La Guajira es una entidad territorial nivel 6, conformada por 8 secretarías y su distribución jerárquica se puede observar en la Figura 4.2. La Secretaría de gobierno es la dependencia encargada de proyectar, dirigir, implementar y controlar las políticas, así como la adopción de proyectos para el orden público, defensa del ciudadano, asuntos electorales, administrativos, atención y prevención de desastres, cultura, talento humano, entre otras funciones adicionales que ejecuta dentro de la municipalidad.

Figura 4.2 Organigrama Alcaldía municipal Villanueva



Actualmente el secretario de Gobierno Municipal es Miguel Ángel López Contreras y cuenta con un total de 16 funcionarios, ubicados en las oficinas adscritas a la secretaría como se observa en la Tabla 4.1.

Tabla 4.1 Distribución funcionarios secretaría de gobierno y jurídica

Oficina	N° de funcionarios
Secretaría de gobierno	3
Talento humano	1
Comisaría de familia	3
Inspección de policía	2
Sistemas	2
Jurídica	5
Total	**16**

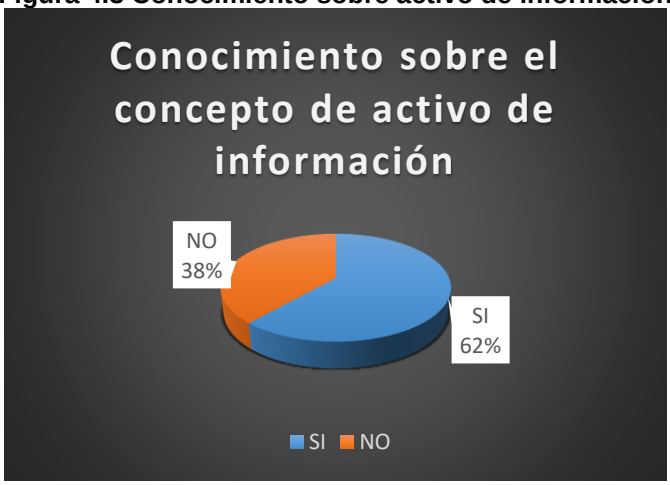
4.1.1. Procesamiento e interpretación de datos

Se realizó una encuesta cerrada en las dependencias adscritas a la secretaría de gobierno municipal con el objetivo de evaluar sus conocimientos en relación a términos informáticos básicos y a los hábitos de cada oficina al realizar actividades rutinarias en sus equipos de trabajo y documentos físicos. La encuesta consta de 30 preguntas de selección múltiple y fueron partícipes el 94% de los funcionarios.

A continuación, se encuentra una interpretación general de las respuestas proporcionadas por los empleados a cada una de las preguntas de la Encuesta de caracterización Que se encuentra en Anexos. Es necesario realizar este tipo de actividades de manera individual debido a que, gracias a la ausencia de controles o políticas por parte de la entidad cada empleado desarrolla habilidades distintas a las del otro, lo que hace necesario un estudio menos generalizado.

Pregunta 1: ¿sabe usted que es un activo de información

Figura 4.3 Conocimiento sobre activo de información



Las respuestas obtenidas en esta pregunta se aprecian en la Figura 4.3, dan como resultado que el 38% de los empleados encuestados no saben que es un activo de información.

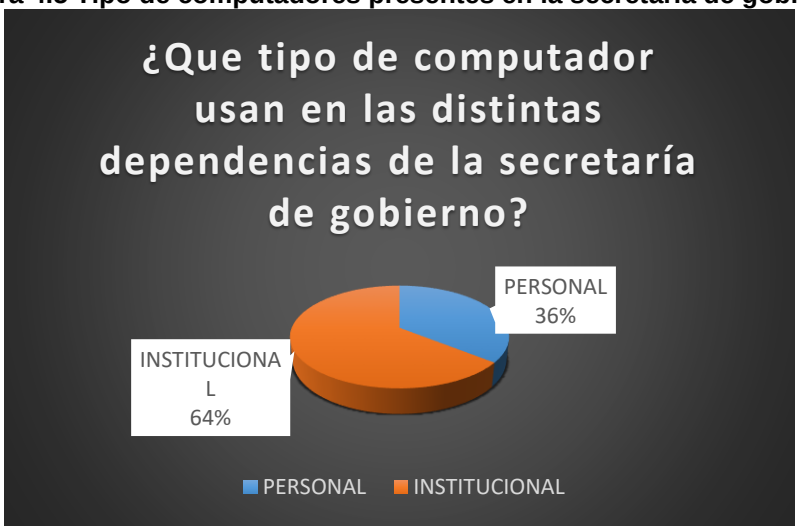
Pregunta 2: ¿conoce usted que es seguridad de la información?

Figura 4.4 Conocimiento de empleados relacionado al concepto de seguridad de la información

Los resultados obtenidos en esta pregunta (ver Figura 4.4), muestran que el 64% de los empleados encuestados reconocen el concepto de seguridad informática, lo cual es importante para el desarrollo del sistema de gestión en la secretaría de gobierno.

Pregunta 3: En el trabajo, ¿Utiliza su computador personal o institucional?

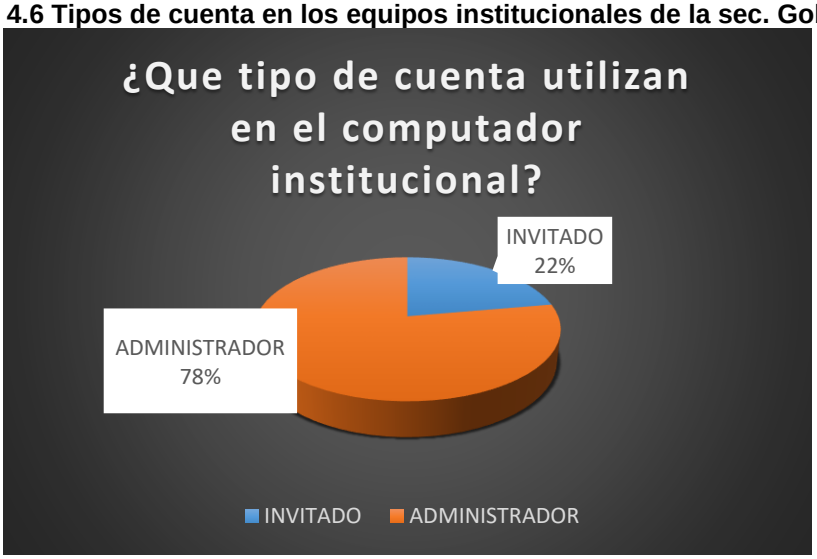
Figura 4.5 Tipo de computadores presentes en la secretaría de gobierno



Los resultados obtenidos en esta pregunta (ver Figura 4.5), muestran que el 64% de los empleados de la secretaría de gobierno emplean un computador institucional para el desarrollo de sus actividades cotidianas.

Pregunta 4: En caso de utilizar un computador institucional, ¿Dispone usted de una cuenta de invitado?

Figura 4.6 Tipos de cuenta en los equipos institucionales de la sec. Gobierno



Los resultados obtenidos en esta pregunta observados en la Figura 4.6, muestran que de ese 64% de personas que tienen equipos institucionales, solo el 22% manejan una cuenta de invitado, lo cual es un factor a tener en cuenta al momento de crear políticas de gestión de riesgos en la secretaría de Gobierno.

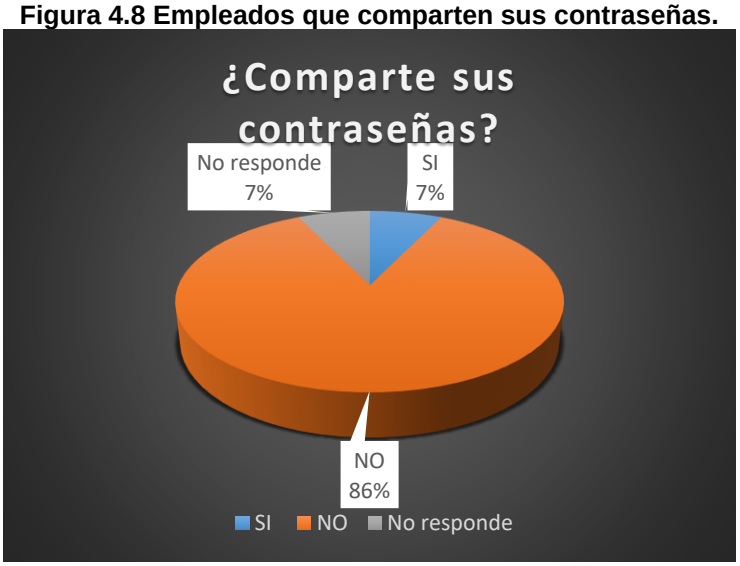
Pregunta 5: ¿Emplea contraseñas para el inicio de sesión?

Figura 4.7 Porcentaje de uso de contraseñas para inicio de sesión

Los resultados obtenidos en esta pregunta, y como se aprecia en la Figura 4.7, muestran una división equitativa, es decir, el 50% de personas utilizan contraseñas en sus equipos; este resultado es de suma importancia y debe ser tenido en cuenta para la creación de políticas internas dentro de la secretaría.

Pregunta 6: ¿Comparte su contraseña con otras personas de la oficina o ajenas a ellas?

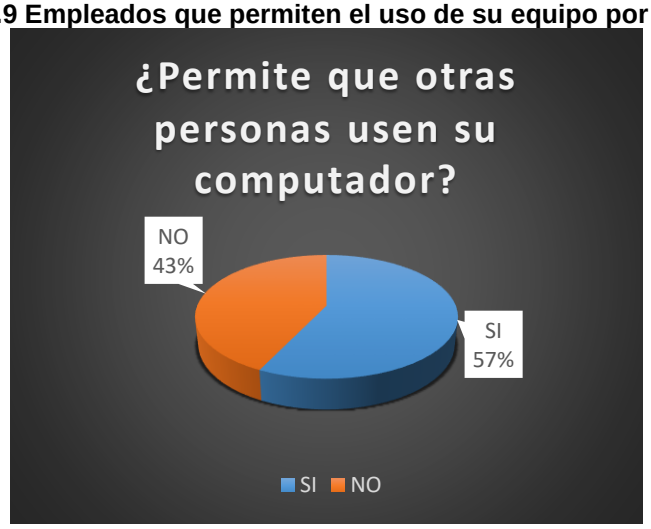
Figura 4.8 Empleados que comparten sus contraseñas.



Los resultados obtenidos en esta pregunta se encuentran representados gráficamente en la Figura 4.8, dan como resultado que el 86% de los empleados no comparten sus contraseñas con otras personas; esto muestra una buena práctica por parte de cada uno de ellos, pero sería ideal que el 100% de ellos no compartan contraseñas.

Pregunta 7: ¿Permite que su equipo lo utilicen otras personas aparte de usted?

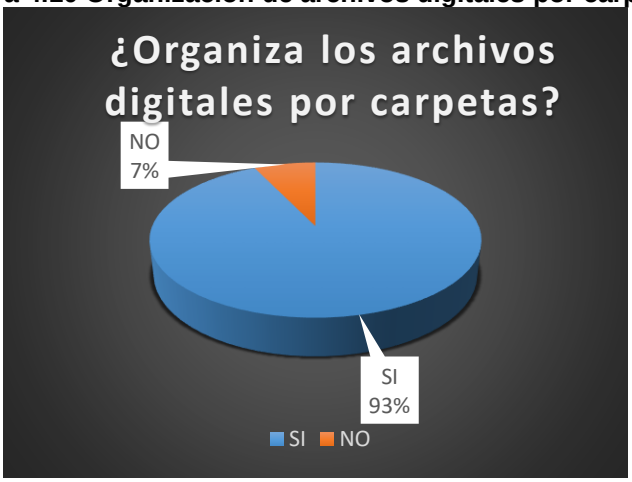
Figura 4.9 Empleados que permiten el uso de su equipo por terceros



Los resultados obtenidos en esta pregunta, los cuales están graficados en la Figura 4.9 muestran que el 57% de las personas permiten que otras personas usen su computador, a pesar que en la pregunta 6 el 86% no comparte sus contraseñas.

Pregunta 8: ¿Organizas los archivos digitales por carpetas según su clasificación?

Figura 4.10 Organización de archivos digitales por carpetas



Los resultados obtenidos en esta pregunta, cuya representación gráfica se observa en la Figura 4.10 muestran que el 93% de los empleados tienen buena práctica relacionada a la organización de los archivos en sus equipos por carpetas, lo cual simplifica el trabajo a la hora de buscar un archivo.

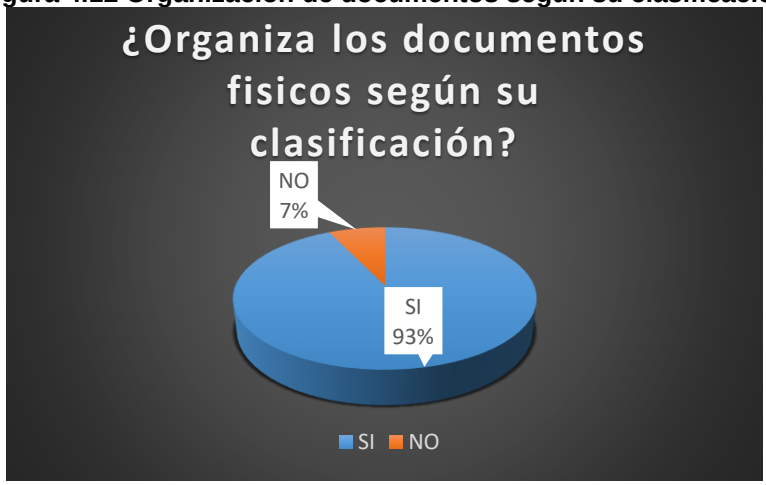
Pregunta 9: ¿Proteges los archivos de información digital con algún cifrado o contraseñas?

Figura 4.11 Seguridad en archivos digitales

Los resultados obtenidos en esta pregunta, los cuales están representados gráficamente en la Figura 4.11 muestran que el 86% de los empleados no protegen los archivos con contraseña, práctica que debe ser impartida por el personal de sistemas con el objetivo de capacitar al personal y aumentar la protección de los activos de información digital.

Pregunta 10: ¿Organizas los documentos físicos por folios, carpetas o por bloques según su clasificación?

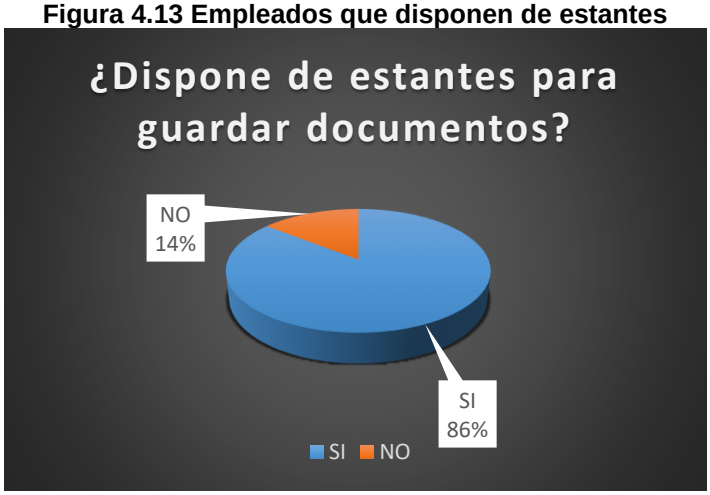
Figura 4.12 Organización de documentos según su clasificación



Los resultados obtenidos en esta pregunta, cuya gráfica se aprecia en la Figura 4.12 muestran que el 93% de los empleados organizan sus archivos físicos por folios de manera clasificada, lo cual, junto con los resultados obtenidos en la pregunta 8 son buenas prácticas y simplifican trabajo a la hora de buscar información.

Pregunta 11: ¿Tiene algún estante para guardar los documentos físicos?

Figura 4.13 Empleados que disponen de estantes



Los resultados obtenidos en esta pregunta y tal como se observa en la Figura 4.13, muestran que el 86% de empleados de la secretaría de gobierno disponen de estantes o lockers para guardar documentos.

Pregunta 12: ¿El estante tiene cerradura/candado en buen estado?

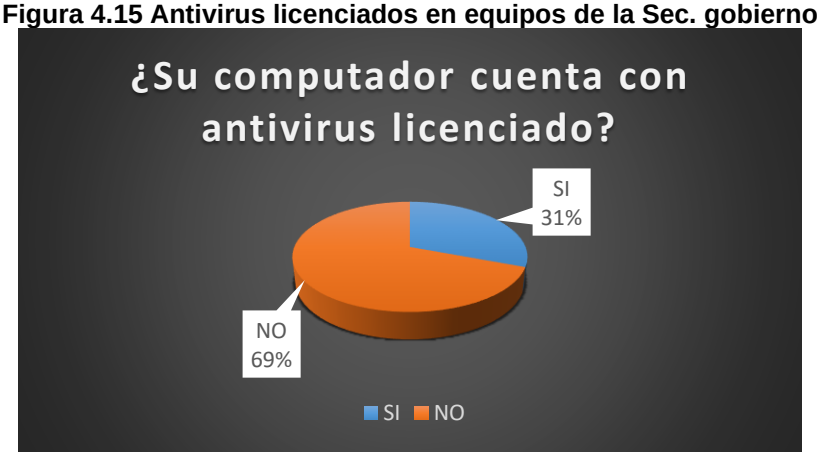
Figura 4.14 Estantes disponibles con cerraduras

A pesar de que el 93% de los empleados organizan y clasifican los documentos, y que el 86% disponen de organizadores o estantes, los resultados obtenidos en esta pregunta, y como se observa en la Figura 4.14 se observa que el 79% de estantes disponibles carecen de buena cerradura, por lo que los activos de

información que se almacenan en estos estarán disponibles para quien quiera observarlo porque carece de protección.

Pregunta 13: ¿Su computador cuenta con antivirus licenciado?

Figura 4.15 Antivirus licenciados en equipos de la Sec. gobierno



Los resultados obtenidos en la presente pregunta, y tal como se observa en la Figura 4.15 muestran que el 69% de los empleados disponen de antivirus licenciado.

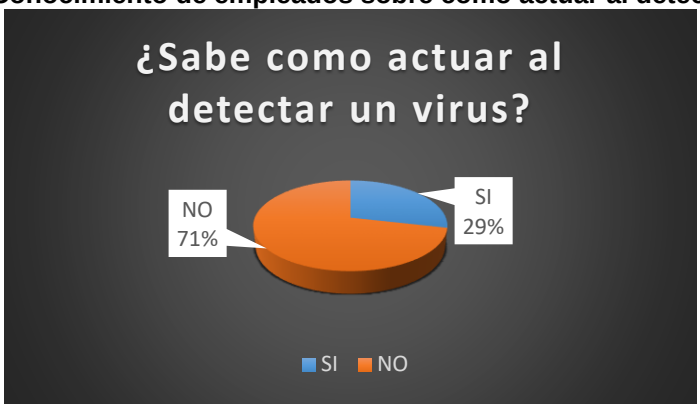
Pregunta 14: ¿Sabe que es un virus informático?

Figura 4.16 Empleados que conocen qué es un virus informático

Los resultados obtenidos en esta pregunta, y como se observa en la Figura 4.16, muestran que el 86% de los empleados de la secretaría de gobierno saben que es un virus informático, el 14% restante de los empleados desconocen el concepto y acción de un virus informático.

Pregunta 15: ¿Tiene conocimiento sobre cómo actuar en caso de detectar un virus?

Figura 4.17 Conocimiento de empleados sobre cómo actuar al detectar un virus.

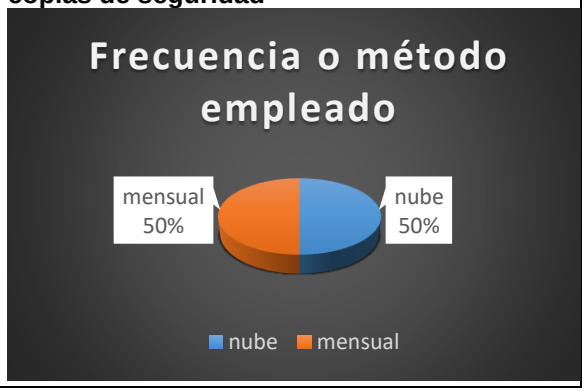


Los resultados obtenidos en la presente pregunta (ver Figura 4.17)muestran que el 71% de la población encuestada no saben cómo actuar al momento de detectar un virus; muchos manifestaron que “simplemente dejaban que su antivirus actuara”.

Pregunta 16: ¿Realiza copias de seguridad de su información de manera periódica? De ser positiva su respuesta, favor indicar cada cuanto lo realiza

Figura 4.18 ¿Realizan copias de seguridad de la información?

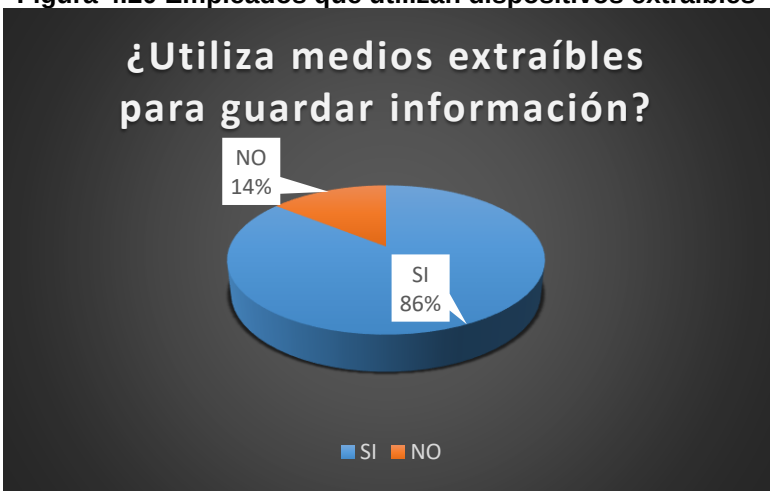
Figura 4.19 Método implementado para copias de seguridad



Los resultados obtenidos en esta pregunta, cuya representación gráfica se observa en la Figura 4.18, muestran una cifra preocupante: el 79% de los encuestados **no realizan copias de seguridad** de la información que poseen en sus equipos y tan solo el 21% de ellos manifiestan hacerlo, uno de ellos lo realiza mensualmente y el otro empleado menciona donde almacena dicha copia (ver Figura 4.19).

Pregunta 17: ¿Introduce memorias, discos duros, o cualquier otro dispositivo extraíble para el intercambio de información?

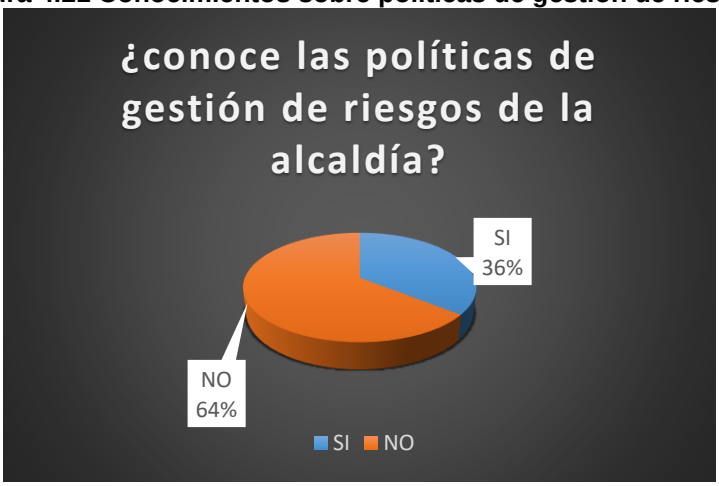
Figura 4.20 Empleados que utilizan dispositivos extraíbles



Los resultados obtenidos en esta pregunta, representado gráficamente por medio de la Figura 4.20 muestran que el 86% de los empleados adscritos a la secretaría de gobierno intercambian información mediante dispositivos extraíbles.

Pregunta 18: ¿Tiene conocimiento acerca de políticas de gestión de riesgos?

Figura 4.21 Conocimientos sobre políticas de gestión de riesgos



Los resultados obtenidos en esta pregunta (ver Figura 4.21) muestran que el 64% de los empleados no conocen la política de gestión de riesgos de la entidad; esto es una respuesta acertada debdo a que en dicha política no existe en la alcaldía y debe ser instaurada para el desarrollo del SGSI.

Pregunta 19: ¿Tiene conocimiento acerca de políticas de tratamiento de información confidencial?

Figura 4.22 Empleados que conocen las políticas de tratamiento de datos

Los resultados obtenidos en esta pregunta (ver Figura 4.22)dan como resultado que el 64% de los empleados conocen las políticas de tratamiento de información de la entidad, las cuales deben aplicarse día a día para la contribución de la seguridad de la información.

Pregunta 20: ¿Tiene conocimiento acerca de políticas de ahorro energético?

Figura 4.23 Conocimiento sobre políticas de ahorro energético

Los resultados obtenidos en esta pregunta (ver Figura 4.23), dan como resultado que el 43% de los empleados conocen las políticas de ahorro energético de la alcaldía, las cuales no están diseñadas o simplemente no existen. Al momento de la socialización de las respuestas estos empleados manifiestan que le llaman

políticas de ahorro energético a las buenas prácticas de ahorro de energía propias de cada uno de ellos.

Pregunta 21: ¿sabe usted si en la entidad existen políticas de seguridad de la información?

Figura 4.24 Conocimiento de empleados relacionado a las políticas de seguridad de la información

Los resultados obtenidos en esta pregunta, observados en la Figura 4.24, muestran que el 57% de empleados no conocen las políticas de seguridad de la información de la alcaldía.

Pregunta 22: ¿Guarda información personal (como fotos, videos, música) dentro de su equipo institucional?

Figura 4.25 ¿Almacenan los empleados información personal en los equipos institucionales?

Los resultados obtenidos en esta pregunta, y tal como se puede apreciar en la Figura 4.25 muestran que el 93% de empleados de la secretaría de gobierno no guardan información personal dentro de los equipos institucionales en los que laboran.

Pregunta 23: ¿Su oficina cuenta con un plan de contingencia de riesgos o desastres (Inundaciones, incendio, alteraciones)?

Figura 4.26 Existencia de plan de contingencia en las oficinas de la Sec. Gobierno

Los resultados obtenidos en esta pregunta, como se observa en la Figura 4.26, muestran que las oficinas adscritas a la secretaría de gobierno no cuentan con planes de contingencia ante riesgos o desastres naturales lo cual es muy preocupante debido a que se compromete la integridad y disponibilidad de cada activo de la información en caso de la ocurrencia de cualquiera de estos eventos.

Pregunta 24: ¿Las puertas y ventanas de su dependencia se encuentran en buen estado?

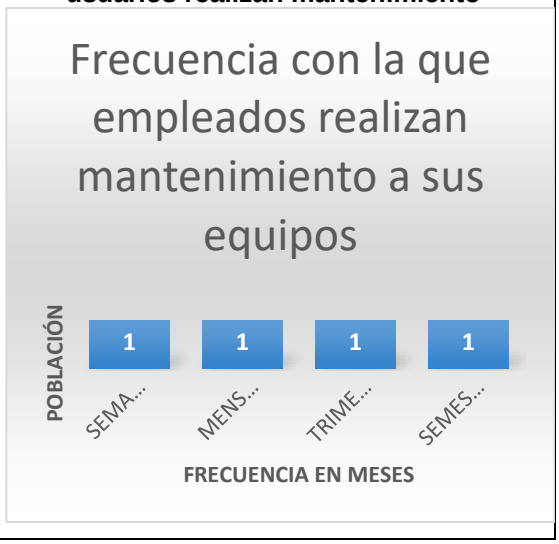
Figura 4.27 Estado de puertas y ventanas de la Sec. Gobierno

Los resultados obtenidos en esta pregunta (ver Figura 4.27), muestran que, a pesar de que el 71% de puertas y ventanas están en buen estado, mientras que el 29% no lo están, por lo que se deben tomar acciones correctivas desde los altos directivos para dar solución a esta problemática.

Pregunta 25: ¿Le realiza mantenimiento preventivo a su equipo? De ser positivo su respuesta, por favor indique cada cuanto tiempo

Figura 4.28 Mantenimiento preventivo y correctivo a los equipos

Figura 4.29 Frecuencia con la que los usuarios realizan mantenimiento



Los resultados obtenidos en esta pregunta, y como se observa en la Figura 4.28 muestran que el 71% de los empleados adscritos a la secretaría de gobierno no realizan mantenimiento preventivo a sus equipos, el 29% de los trabajadores que si realiza mantenimiento preventivo indican en la **Figura 4.29** la frecuencia con que lo hacen.

Pregunta 26: ¿Sabe usted qué es un delito informático?

Figura 4.30 Conocimiento de los empleados sobre delito informático

Las respuestas obtenidas en esta pregunta (Figura 4.30), muestran que el 86% de los empleados tienen conocimiento acerca de lo que es un delito informático.

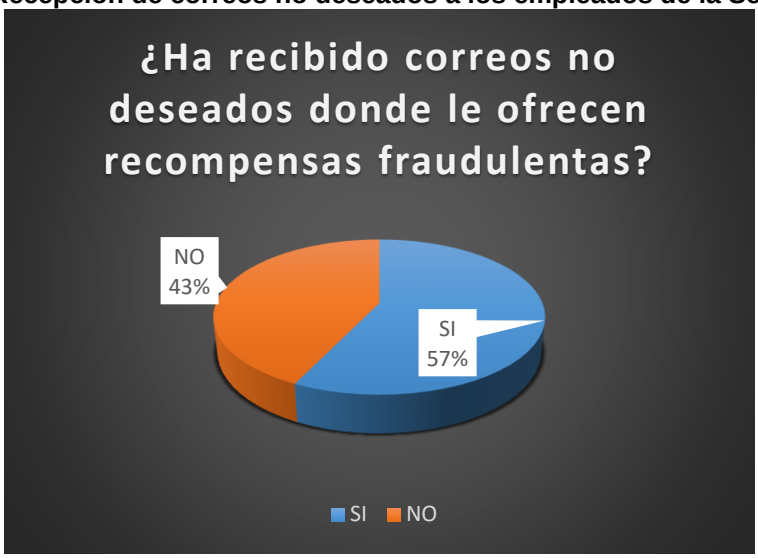
Pregunta 27: ¿Sabe que es Phishing?

Figura 4.31 Conocimiento de los empleados sobre Phising

Las respuestas obtenidas en la presente pregunta, representada gráficamente en la Figura 4.31, dan como resultado que el 72% de los empleados de la secretaría de gobierno no saben que es phishing, mientras que un 21% sí.

Pregunta 28: ¿Ha recibido correos no deseados, sospechosos o fraudulentos, donde le ofrecen algún tipo de recompensa o premio?

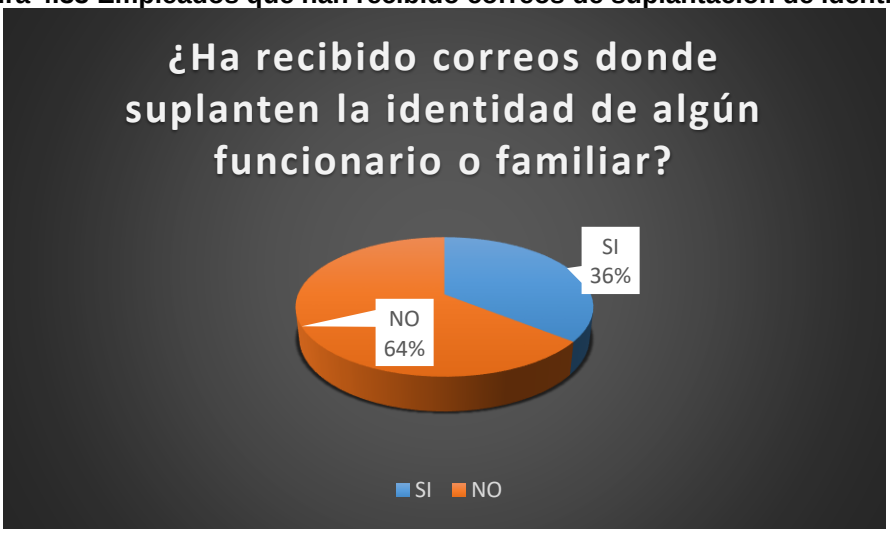
Figura 4.32 Recepción de correos no deseados a los empleados de la Sec. Gobierno.



Los resultados obtenidos en la presente pregunta, representada gráficamente en la Figura 4.32 dan como resultado que más del 50% de los empleados de la secretaría de gobierno han recibido correos engañosos; los correos engañosos o fraudulentos son una técnica de phishing en donde por medio del engaño se ganan la confianza de sus víctimas para poder obtener datos mediante la ingeniería social.

Pregunta 29: ¿Ha recibido correos donde suplanten la identidad de algún funcionario o familiar?

Figura 4.33 Empleados que han recibido correos de suplantación de identidad



Los resultados obtenidos en la presente pregunta y como se observa en la Figura 4.33,muestran que un 36% de los empleados de la secretaría de gobierno han recibido correos de suplantación de identidad, lo cual es otra técnica empleada en el phishing

Pregunta 30: ¿Tiene libertad para instalar aplicaciones, programas o cualquier tipo de software en su equipo de trabajo?

Figura 4.34 Libertad para la instalación de software en equipos institucionales

Los resultados obtenidos en esta pregunta (ver Figura 4.34) muestran que el 64% de los empleados de la secretaría de gobierno tienen libertad para instalar aplicaciones en sus equipos, actividad que no es controlada debido a que el 78% de los funcionarios que emplean equipos institucionales trabajan en la cuenta de administrador y no en una de usuario (ver Figura 4.6 Tipos de cuenta en los equipos institucionales de la sec. Gobierno), teniendo a su disposición el equipo para realizarle tantos cambios como crean conveniente.

4.1.2. Análisis.

Según los resultados obtenidos en la encuesta, concuerdan con lo visto al realizar actividades de verificación en cada dependencia, donde se observaron las prácticas de cada empleado, manejo de activos y control de información confidencial, así como del estado de la planta física de las oficinas adscritas a la secretaría de gobierno municipal. Los resultados no son satisfactorios porque aún hay falencias, pero con la instauración de políticas y socialización de temáticas se contribuye al mejoramiento de conocimientos convertidos en prácticas correctas para disminuir el impacto y probabilidad de ocurrencia de ataques que vulnere los activos de información.

4.2. Inventario de activos de información

Una vez realizadas las actividades anteriores, y disponer de un inventario de activos de información, es recomendable realizar una clasificación de los mismos como se observa en la ***Tabla 4.2 Encabezado de Inventario y clasificación de activos*** de información. La clasificación de inventario debe ser preciso, consistente y ajustado a la realidad de las dependencias. Consiste en identificar el tipo de información presente en el inventario tales como infraestructura, conocimientos de los empleados información digital e impresa. La clasificación se puede organizar en varias secciones:

- ✓ **Según su clasificación de acceso:**
  - Acceso exclusivo
  - Acceso ilimitado
  - Costo de recuperación (material, económica, tiempo)
- ✓ **Según la magnitud del daño:**
  - Bajo
  - Medio
  - Alto

Tabla 4.2 Encabezado de Inventario y clasificación de activos de información

Elementos	Clasificación			Magnitud del daño		
Selecciona el tipo de activo de información	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material)	Bajo	Medio	Alto

Basados en la definición de inventario y activo de información de la norma ISO/IEC 27001 donde se define a este último como cualquier cosa que tenga valor para la organización; en la Tabla 4.3,Tabla 4.4 y Tabla 4.5 se definieron los siguientes activos para la secretaría de gobierno de la alcaldía municipal de Villanueva la guajira.

Tabla 4.3 Inventario de activos de información según tipo de datos o información

Elementos	Clasificación del activo de información			Magnitud del daño		
Datos o información	**Confidencial, contenido sensible.**	**Leyes, decretos, contratos o convenios**	**De empleados, o involucran a la institución**	**Bajo**	**Medio**	**Alto**
Documentos institucionales (Proyectos, Informes, reportes)	SI					
Recursos Humanos	SI					
Directorio privado de contactos	SI					
Contratos y cuentas de cobro	SI					
Material de producción institucional tales como: Folletos, Pancartas, Pendones.		SI				
Teléfono			SI			
Red de cableado interna (intranet)			SI			
Finanzas		SI				
Planos de cableado de red informática	SI					

Procesos, seguimiento a empleados	SI					
Decretos		SI				
Correo electrónico			SI			
Página web institucional			SI			
Respaldos de información alojada en página web	SI					
Expedientes	SI					
Base de datos interna			SI			

Tabla 4.4 Inventario de activos de información según tipo de sistema o infraestructura

Elementos	Clasificación			Magnitud del daño		
Sistemas e infraestructura	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material)	Bajo	Medio	Alto
Routers			SI			
Switch			SI			
Acces point			SI			
Servidores	N/A	N/A	N/A			

Computador institucional de escritorio		SI				
Computador institucional portátil		SI				
Computador portátil personal	SI					
Impresoras		SI				
Escáner		SI				
Celulares	SI					
Oficinas			SI			
Vehículos	SI					

Tabla 4.5 Inventario de activos de información según personal por oficinas adscritas a la secretaría de gobierno municipal

Elementos de información	Clasificación			Magnitud del daño		
Personal	**Persona de alto perfil / referente de la institución**	**Persona experta en su área de desempeño**	**Perfil bajo, no indispensable para el funcionamiento de la institución**	**Bajo**	**Medio**	**Alto**
Secretario de Gobierno	SI					
Inspector de policía	SI					

Comisaria de familia	SI					
Personal técnico						
Administración		SI				
Sistema/Soporte técnico		SI				
Servicios generales		SI				

Capítulo 5

PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

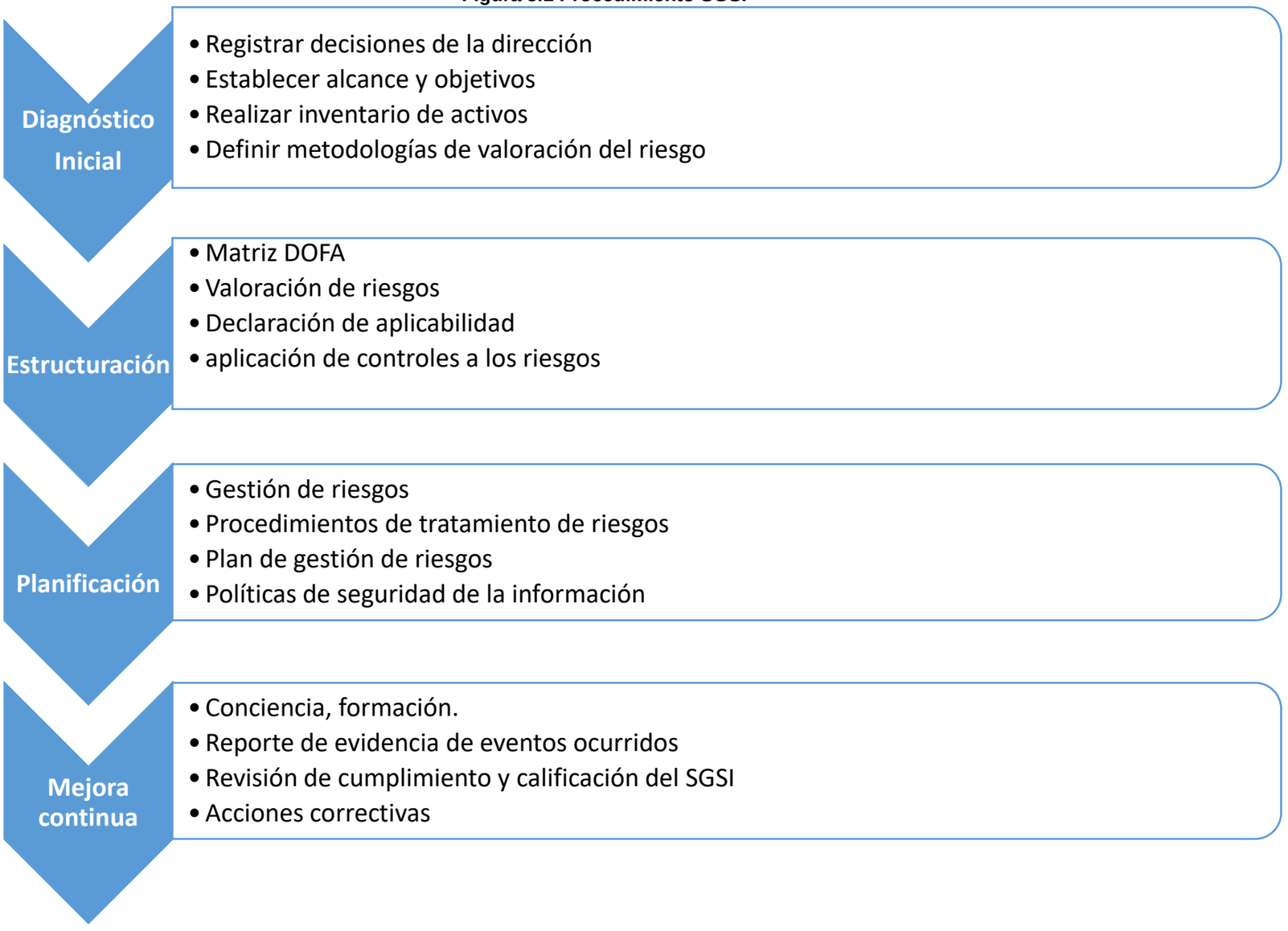
5.1 Modelo del Sistema de gestión de seguridad de la información 42
5.2 Fases del modelo del SGSI 44
5.3. Evaluación de los controles de la norma ISO/IEC 27001 49
5.4. Fase 3: Planificación del sistema 52

5.1. Modelo del Sistema de gestión de seguridad de la información

La norma ISO/IEC 27001 ha sido diseñada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión (ICONTEC, 2006), en donde la decisión de la implementación debe ser estratégica para las organizaciones, debido a que dicho sistema debe estar orientado a todas las necesidades de la empresa o entidad para así ajustar los objetivos en búsqueda la implementación de mejores controles y políticas de seguridad para los empleados y la entidad misma. Es por eso que para un funcionamiento ideal se deben identificar muchos procesos (el enfoque del SGSI es basado en procesos), es decir, identificar tantas actividades como sea posible que se puedan gestionar entre sí para que las soluciones de esa actividad sean tenidas en cuenta como la entrada de la siguiente, lo cual estimularía a la mejora continua de dicho sistema midiendo los objetivos planteados con anterioridad.

5.1.1. Modelo general del SGSI

Figura 5.1 Procedimiento SGSI



Fuente: propia

5.2. Fases del modelo del SGSI

En concordancia al marco de referencia de la norma NTC-ISO/IEC 27001 para el diseño del sistema de gestión de seguridad de la información en la alcaldía municipal de Villanueva la Guajira, se establecen 4 fases como se observa en la Figura 5.2 Fases para el desarrollo e implementación del SGSI:

Figura 5.2 Fases para el desarrollo e implementación del SGSI

Para la primera fase, llamada **Diagnóstico inicial** se identificó el nivel de la entidad en relación al modelo de seguridad de la información, inspeccionando la información disponible, realizando preguntas a los empleados (especialmente a los de la dependencia donde se estará implementando), esto con el objetivo de observar sus conocimientos en cuanto al sistema de gestión existente en la entidad y el dominio de cada uno de ellos respecto al tema.

En la fase de **estructuración**, se determinará el contexto y expectativas para generar el alcance del sistema de gestión, además de establecer límites, políticas generales y objetivos.

En la fase de **planificación** se establece la identificación, valoración, tratamiento de todas las vulnerabilidades identificadas en las dependencias, activos

de información, políticas para la protección de distintas áreas, y los respectivos controles por cada vulnerabilidad encontrada.

En la fase de **Mejora continua** se identificarán acciones que contribuyan al mejoramiento del sistema de gestión, ajuste de las políticas y calificar la madurez del sistema. Esta fase se desarrollará en el capítulo 7: ***PLAN DE MEJORA CONTINUA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN***

5.2.1. Fase 1: Diagnóstico inicial

Esta fase, es la que ha sido implementada en el capítulo **4**: **IDENTIFICACIÓN DE ACTIVOS Y FUENTES DE INFORMACIÓN,** donde se realizó una evaluación de las habilidades o dominio que tienen las personas dentro de la entidad con respecto a la seguridad de la información (en adelante S.I); cabe resaltar que no se solicitó documentación de planes anteriores debido a que no se ha implementado el sistema de gestión anteriormente, es por eso que solo se realizó un cuestionario de treinta preguntas orientadas al tema de S.I

En resumen, el procedimiento ejecutado en esta fase fue el siguiente:

- Entrevistas con cada jefe de las dependencias adscritas a la secretaría de Gobierno municipal, su nombre es Miguel Ángel López
- Cuestionario con treinta preguntas relacionadas con S.I, y actividades de rutinas a los empleados de la secretaría.
- Revisión de la misión, visión, objetivos de la alcaldía y de la secretaría en específico, políticas, procedimientos, normatividad existente.
- Verificación de las respuestas obtenidas en el cuestionario
- Inventario de activos de información.

5.2.2. Metodología de valoración de riesgo y estimación de niveles de riesgos

Según el alcance y los objetivos de la gestión del riesgo se recomienda el desarrollo de criterios para evaluar el riesgo que tenga como objetivo determinar el riesgo en seguridad de la información propios de la entidad siguiendo los siguientes ítems:

- ✓ El grado de criticidad de cada activo de información inventariado.
- ✓ Obligaciones contractuales de la dependencia
- ✓ La importancia de la disponibilidad, confidencialidad e integridad de la información dentro de un proceso de seguridad de la información
- ✓ Criterios de impacto de riesgo, los cuales se implementan para la especificación de prioridades en la valoración del riesgo.

5.2.2.1 Criterios de impacto de riesgo

Los criterios de impacto de riesgo son importantes debido a que son específicos respecto a términos del grado de daño para la entidad, causados por cualquier evento que comprometa la seguridad de la información teniendo en cuenta los siguientes aspectos:

- ✓ Nivel de clasificación de los activos de información
- ✓ Brechas en seguridad donde se comprometa la disponibilidad, integridad o confidencialidad de la información
- ✓ Deterioro de los procesos establecidos y recaiga directamente en la reputación de la dependencia.

5.2.2.2 Criterios de aceptación de riesgo

Los criterios de aceptación de riesgo podrían ser definidos como la relación entre el beneficio deseado y la estimación del riesgo de la dependencia, dependiendo de las políticas, metas y objetivos de la entidad; es por esa razón que

en las oficinas adscritas a la secretaría de gobierno se deben definir unas escalas propias para los niveles de aceptación del riesgo teniendo en cuenta que pueden incluir un umbral de nivel de riesgo deseable, y que los riesgos que lo sobrepasen puedan ser aceptados por la alta dirección según un estudio previamente realizado.

En síntesis, la valoración del riesgo realiza una estimación de las posibles manifestaciones de riesgos que pueden comprometer las dependencias y afectar de manera directa la confidencialidad, integridad y disponibilidad de la información.

Según la probabilidad de ocurrencia los criterios de valoración se definen de la siguiente manera (ver Tabla 5.1):

Tabla 5.1 Tabla probabilidad con la que pueden ocurrir los riesgos

Escala de Valoración	Valoración	Descripción
1	**Raro**	El evento puede ocurrir en algunas circunstancias, y en los últimos 5 años no se ha presentado
2	**Improbable**	El evento podría ocurrir en cualquier momento, y en los últimos 5 años por lo menos ha ocurrido 1 vez
3	**Posible**	El evento podría ocurrir en cualquier momento, y en los últimos 2 años por lo menos ha ocurrido 1 vez
4	**Probable**	El evento puede ocurrir en el 75% de las circunstancias, puesto que ha sucedido al menos 1 vez en el último año
5	**Casi seguro**	Se espera que este evento ocurra en el 90% de las circunstancias, debido a que es común

		que ocurra en repetidas ocasiones durante el año.

Según el impacto que tenga el riesgo en la entidad se clasifican de la siguiente manera (ver Tabla 5.2):

Tabla 5.2 Tabla de impacto en caso de incidentes de seguridad de los activos de información

Escala de Valoración	Valoración	Descripción
1	**Insignificante**	La ocurrencia del evento no tendría consecuencias relevantes para la dependencia donde se presente.
2	**Menor**	La ocurrencia del evento implicaría realizar ajustes en los procedimientos del proceso dentro de la dependencia donde se presente.
3	**Moderado**	Si el evento llegase a ocurrir, afectaría la credibilidad o imagen de todos los funcionarios y contratistas de la dependencia, produciendo incluso consecuencias legales.
4	**Mayor**	Si el evento llegase a ocurrir, tendría afectaciones a nivel estratégico, presentando dificultades o intermitencias en las operaciones de los procesos.
5	**Catastrófico**	Si el evento llegase a ocurrir, tendría un impacto no deseado en la confidencialidad, integridad y disponibilidad de la información, lo cual pone en riesgo la reputación/imagen de la

		dependencia e incluso sanciones por parte de un ente de control.

4.2.2.3 Mapa de evaluación del riesgo

Se hace de forma cualitativa comparando la probabilidad de ocurrencia del riesgo contra el impacto, lo que da como resultado una matriz observada en la Tabla 5.3, así como las zonas de riesgo con sus respectivas formas de tratamiento de cada riesgo:

Tabla 5.3 Mapa de evaluación, relación probabilidad/impacto

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Raro	B	B	M	A	A
Improbable	B	B	M	A	E
Posible	B	M	A	E	E
Probable	M	A	A	E	E
Casi Seguro	A	A	E	E	E

Fuente: Guía de riesgos DAFP

Zonas de riesgo:

- ✓ Zona de riesgo Baja (B): Asumir el riesgo.
- ✓ Zona de riesgo Moderada (M): Asumir el riesgo, Reducir el riesgo.
- ✓ Zona de riesgo Alta (A): Reducir el riesgo, evitar, compartir o transferir.
- ✓ Zona de riesgo Extrema (E): Reducir el riesgo, evitar, compartir o transferir.

5.3. Evaluación de los controles de la norma ISO/IEC 27001

En esta etapa, se debe determinar la aplicación o no de los 114 controles del Anexo A de la norma ISO/IEC 27001, este documento es conocido como

declaración de aplicabilidad; la finalidad de esta declaración es describir los objetivos de control y controles pertinentes y aplicables para el SGSI de la organización (ICONTEC, 2006). La exclusión de cualquier control establecido en el anexo A de la norma es permitida, siempre y cuando se justifique su exclusión para así validar que ningún control se omitió de manera involuntaria.

Se debe resaltar que este documento se realiza luego del tratamiento de riesgos y un ejemplo del formato es el que se observa en la Tabla 5.4;

Tabla 5.4 Encabezado declaración de aplicabilidad SGSI

Estado y aplicabilidad de controles de seguridad de la información				
Sección	**Controles de seguridad de la información**	**Estado**	**Preguntas**	**Comentarios**

Donde:

- ✓ **Sección:** contiene la sección perteneciente a cada uno de los 114 controles del anexo A, con sus respectivas subsecciones.
- ✓ **Controles de seguridad de la información:** Contiene la descripción de cada control por secciones.
- ✓ **Estado:** Aquí se establece en qué estado se encuentra cada control, si se aplica o no, y en qué nivel lo encontramos. Esta escala de clasificación se divide en:
  - **Desconocido:** se clasifica como **desconocido** cuando el control no ha sido verificado por el consultor o encargado de la implementación del SGSI.
  - **Inexistente**: es cuando no se lleva a cabo el control de seguridad en los sistemas de información.

- **Inicial:** Existen, pero no se gestionan dichos controles, o simplemente no existe un proceso formal para realizarlos.
- **Repetible:** La medida de seguridad se realiza de un modo informal, esto es implementando procedimientos propios, dejando la responsabilidad de cumplimiento de dicho control a cada uno de los empleados.
- **Definido**: El control se aplica conforme a un procedimiento documentado que no ha sido aprobado por la alta dirección.
- **Administrado**: El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado por la alta dirección y formalizado.
- **Optimizado**: El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y la eficacia de dichos controles se mide por indicadores periódicos.
- **No aplicable:** Cuando el control no se ajusta a los intereses de la organización, o simplemente no se tendrán en cuenta por otros motivos y han sido ignorados por la administración.

✓ **Preguntas:** Preguntas establecidas para realizar a la persona a cargo de cada dependencia adscrita a la secretaría de gobierno.

✓ **Comentarios**: Espacio para refutar, argumentar o justificar en cualquier control, especialmente en los que no se van a implementar.

5.3.1. Fase 2: Estructuración del sistema de gestión

En la etapa de estructuración del SGSI, la dependencia determina los factores internos y externos que generan algún impacto para cumplir con los resultados planificados en el sistema de gestión. La metodología sugerida a implementar en esta etapa es un análisis DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas) para así conocer gran parte de los riesgos externos.

5.4. Fase 3: Planificación del sistema

5.4.1. Gestión de riesgos de seguridad de la información

Toda la temática de riesgos ocupa una porción considerable dentro de la ejecución del SGSI, principalmente porque las organizaciones deben seleccionar mecanismos para identificar, evaluar, clasificar y ejecutar estrategias para poder reducirlos hasta niveles mínimos; al planificar buenas técnicas y que estas sean implementadas por los empleados, directivos y jefes disminuye radicalmente las probabilidades de comprometer la confidencialidad, integridad y disponibilidad de cada activo de la información presente en la empresa. A continuación, se presenta el modelo basado en el ciclo Deming o PHVA que debe ser aplicado a todos los procesos y a los servicios de cualquier sistema dentro de las dependencias tal como se observa en la Tabla 5.5.

Tabla 5.5 Criterios PHVA en la planificación del SGSI en la secretaría de gobierno municipal

CICLO	ACTIVIDAD
P	Generación de directrices y normas sobre cómo gestionar los riesgos, valorarlos, tratarlos dentro de la implementación conjunta de controles de seguridad de la información
	Planear acciones para el tratamiento de riesgos de seguridad de la información
H	Implementación de acciones para el tratamiento de riesgos y controles de S.I ISO/IEC 27001
	Garantizar la disponibilidad de evidencias suficientes donde se observen resultados del sistema de gestión
	Autoevaluar la robustez de las acciones implementadas en el tratamiento de los riesgos presentados en la entidad
V	Calificar eficacia de las acciones tomadas para tratar cada riesgo presentado en la entidad

	Garantizar que el SGSI cumpla los objetivos definidos anteriormente por la alta dirección respecto al análisis, valoración y respectivo tratamiento de cada riesgo
A	Desarrollar acciones de mejora continua del sistema de gestión orientados a la reducción de brechas de seguridad de la información y así garantizar tanto la disponibilidad, integridad y confidencialidad de la información como una buena reputación; de lo contrario recurrir al rediseño de controles.

5.4.2. Políticas y controles adicionales de seguridad de la información

Toda entidad que desee implementar un SGSI debe contar con unas políticas en relación con el uso de recursos y activos de información. Algunas de estas son obligatorias de acuerdo al Anexo A de la ISO/IEC 27001, así como otras no, pero también son de gran importancia a la hora de la gestión de recursos o para cumplir algunos requisitos con los usuarios o clientes (política anticorrupción, por ejemplo), entre otras políticas más. Estas políticas son:

- ✓ Plan de tratamiento de riesgos.
- ✓ Política anticorrupción.
- ✓ Política de uso de internet.
- ✓ Política de contraseña segura.
- ✓ Política de transferencia de activos de información digital.
- ✓ Política de derechos de autor.
- ✓ Política de uso de software legal.
- ✓ Política de uso de controles criptográficos.
- ✓ Política de seguridad en sistemas físicos.
- ✓ Política de escritorio y pantalla limpia.
- ✓ Política de respaldo de información.
- ✓ Política de uso de correo electrónico.

Capítulo 6

PLAN DE TRATAMIENTO DE RIESGOS Y METODOLOGÍA DE APLICACIÓN DE CONTROLES DEL SGSI

6.1 Plan de tratamiento de riesgos en la secretaría de gobierno municipal 54
6.2 Aplicación de controles Anexo A ISO/IEC 27001.....61

6.1 Plan de tratamiento de riesgos en la secretaría de gobierno municipal

6.1.1 Política de seguridad SGSI

Implementar el SGSI en una entidad exige el establecimiento e implementación del plan de tratamiento de riesgos, donde el objetivo principal es evitar, controlar, transferir y mitigar los eventos de riesgos detectados dentro de cada oficina. En el plan anteriormente mencionado se establece la reglamentación necesaria para garantizar los pilares de la seguridad de la información, es decir, la disponibilidad, confidencialidad e integridad de los activos; por lo tanto, esta política debe ser comunicada y socializada a todos los empleados de las oficinas donde se está implementando el sistema.

6.1.2 Objetivo

Establecer normas generales para garantizar la disponibilidad, integridad y confidencialidad de los activos de información en las oficinas adscritas a la secretaría de gobierno de la Alcaldía Municipal de Villanueva la Guajira

6.1.3 Alcance

Esta política aplica para todos los empleados de las dependencias adscritas a la secretaría de gobierno municipal.

6.1.4 Desarrollo

En la secretaría de gobierno del municipio de Villanueva son conscientes de que la información es un recurso vital para el normal y correcto funcionamiento de cada una de sus dependencias día a día, por lo tanto, se preocupan por preservar la integridad, confidencialidad y disponibilidad de los activos, así como se comprometen a:

- ✓ Desarrollar un plan de concienciación sobre seguridad de la información para cada uno de los funcionarios, independientemente de su cargo o labores que realicen.
- ✓ Implantar políticas, estándares y procedimientos para la protección de la información presente en cada oficina.

La oficina de sistemas, dependencia adscrita a la secretaría de gobierno municipal, en mutuo acuerdo con la alta dirección que en este caso es el secretario de gobierno municipal establecen que:

6.1.4.1 Uso adecuado de los activos de información y acuerdos de confidencialidad

- ✓ La información se debe clasificar según su valor y grado de criticidad de la siguiente manera: pública, clasificada o reservada, y es responsabilidad de cada funcionario.
- ✓ Realización de inventarios de activos de información disponibles, donde se deben incluir los activos físicos mencionando su clasificación, ubicación y propietario(s) designado(s) y actualizarse por lo menos mensualmente.

- ✓ Todos los funcionarios pertenecientes a las oficinas de la secretaría de gobierno deben firmar un acuerdo de confidencialidad antes de tener acceso a los mismos.
- ✓ Al finalizar lazos contractuales entre la alcaldía municipal y uno de los empleados de las distintas oficinas pertenecientes a secretaría de gobierno municipal, y antes de asignar el equipo de cómputo empleado por este a un nuevo usuario, la oficina de sistemas debe asegurarse de respaldar completamente la información y posteriormente se deberá eliminar del equipo.
- ✓ El funcionario saliente debe asegurar que toda la información institucional independientemente del grado de confidencialidad permanece en el equipo y no existen copias no autorizadas de la misma. En caso de existir otras copias, el funcionario debe devolver todo tipo de información que posea resguardada.
- ✓ El funcionario entrante debe firmar un acta de entrega de equipo, donde se enuncie estado, rendimiento y aplicaciones instaladas en el equipo
- ✓ Implementar auditorías internas para verificar cumplimiento de la política establecida

6.1.4.2 Acceso a internet

- ✓ El uso de internet debe ser para fines institucionales y no para realizar otras actividades personales o con fines de lucro
- ✓ Implementar por parte de la oficina de sistemas bloqueo de sitios web innecesarios, debido a que estos consumen recursos de red.
- ✓ No permitir la instalación de archivos o programas no autorizados

6.1.4.3 Correo electrónico

- ✓ El correo electrónico institucional debe ser utilizado únicamente con fines laborales, y queda prohibido el uso de la cuenta para las siguientes actividades:
    - Anunciar, enviar o emitir contenido del cual no se tiene reglamentación, así como información confidencial propia de su puesto de trabajo
    - Enviar correos no deseado (SPAM)
    - Adjuntar archivos que contengan virus, programas con ejecutables o cualquier otro software que pueda interrumpir el correcto funcionamiento del sistema.
    - Generar correos electrónicos suplantando otras personas sin su debida autorización.
- ✓ No acceder al correo electrónico institucional desde conexiones públicas que sean inseguras
- ✓ El correo electrónico institucional de cada dependencia debe ser administrado por una sola persona.

6.1.4.4 Recursos electrónicos y de red.

- ✓ El jefe de sistemas autorizado por el secretario de gobierno debe establecer mecanismos de control, monitoreo y seguridad para el uso de correo electrónico institucional, acceso a sitios sin certificados vigentes de seguridad o con orígenes sospechosos.
- ✓ Se deben realizar análisis de vulnerabilidades de la red interna para verificar la robustez de la red ante un ataque externo
- ✓ La instalación, configuración o formateo de los equipos de cómputo institucionales debe ser realizada por el personal de sistemas.
- ✓ Mantener actualizados los antivirus.

- ✓ Solo los equipos autorizados pueden ser conectados a la red de la alcaldía
- ✓ Para realizar conexión remota debe ser autorizado por el secretario de gobierno y por el jefe de sistemas

6.1.4.5 Control de acceso físico

- ✓ Se debe llevar un control al registro de funcionarios a quienes se les otorguen permisos especiales o privilegios de acceso, los cuales deben revisarse periódicamente

6.1.4.6 Gestión de contraseñas

- ✓ Las contraseñas deben ser cambiadas mensualmente (a excepción de la contraseña de acceso a la red wifi que debe ser cambiada quincenalmente), en caso de sospechar o detectar actividad inusual dentro de las cuentas de correo electrónico institucional, equipos institucionales o en la red wifi deben ser cambiadas inmediatamente.
- ✓ Todos los equipos deben poseer contraseñas de inicio de sesión, esta clave de usuario debe ser única para cada empleado. Las contraseñas deben tener una longitud mínima de 8 caracteres, combinando caracteres alfanuméricos y ser cambiadas mensualmente.
- ✓ Las contraseñas deben ser entregadas almacenadas de forma segura. Abstenerse de guardarlas en su navegador o enviarlas por correo electrónico u otras aplicaciones de mensajería instantánea.
- ✓ Evitar la unificación de contraseñas y masificar el uso de administradores de contraseñas.

6.1.4.7 Protección de los equipos y uso de los equipos institucionales

- ✓ Mejorar por parte de la alcaldía el estado de las instalaciones o de la infraestructura tales como puertas, ventanas, paredes y techos.
- ✓ Es responsabilidad de cada usuario las actividades realizadas a través de su cuenta.

- ✓ Está prohibido ingresar a las áreas de trabajo o extraer de ellas medios extraíbles sin la autorización del jefe inmediato.
- ✓ La salida de equipos de cómputo de las oficinas debe ser autorizada por el secretario de gobierno.
- ✓ Los funcionarios no deben tener privilegios de administrador en los equipos de cómputo institucionales, con el objetivo de evitar modificaciones a las configuraciones establecidas por la oficina de sistemas.
- ✓ El usuario debe bloquear la sesión de su equipo una vez levantado del puesto de trabajo, y apagado al momento de terminar el horario laboral.
- ✓ Implementar el uso de estabilizadores, UPS o reguladores de voltajes teniendo en cuenta que en el municipio se presentan fallas constantes en el servicio de energía eléctrica.
- ✓ No se puede realizar eliminación, modificación o cambio de software ni equipos sin autorización previa.
- ✓ Dotar las instalaciones de equipos de emergencia contra incendios, inundaciones, explosiones o cualquier tipo de desastre o fenómenos meteorológicos.

6.1.4.8 Copias de seguridad

- ✓ Concientizar a los empleados de adoptar la cultura de realización de copias de seguridad y respaldo de información periódicamente y almacenarla en mínimo dos dispositivos distintos.
- ✓ Los medios donde se alojen copias de seguridad deben estar protegidos por contraseña para garantizar la confidencialidad e integridad de la información que allí reposa.

6.1.4.9 Cultura de escritorios y pantallas limpias

- ✓ El escritorio del equipo trabajo debe mantenerse despejado, ya que la sobrecarga de este o mantener muchos archivos, aplicaciones en el inicio afecta radicalmente en el consumo de la memoria RAM.
- ✓ Mantener con seguro los cajones del escritorio
- ✓ No permitir el uso de los equipos por terceros.
- ✓ No anotar contraseñas en lugares visibles.

6.1.4.10 Uso de dispositivos móviles

- ✓ Mantenerlos protegidos con contraseña.
- ✓ El teléfono es de uso personal e intransferible, no permita que otras personas lo utilicen.

6.1.4.11 Recursos humanos

- ✓ Socializar la política de gestión de riesgos con todo el personal.
- ✓ Tener el compromiso de la alta dirección respecto a cumplimiento de las políticas de seguridad establecidas.
- ✓ El funcionario entrante debe recibir un programa de inducción donde sean presentadas las políticas y las sanciones vigentes.
- ✓ Todo el personal debe ser capacitado constantemente en temas de seguridad de la información. Esto es importante debido a que un personal preparado en estos temas contribuye a la protección de la información y disminuye los riesgos de padecer ataques a la seguridad.

6.1.4.12 Políticas de software

- ✓ Regular la instalación de aplicaciones en los equipos de trabajo.
- ✓ Implementar control de prevención y detección de aplicaciones maliciosas.

6.1.5 Sanciones

Cualquier funcionario que se no cumpla o viole esta política será sujeto a medidas disciplinarias, la cual será notificada ante el secretario de gobierno y al jefe de Talento humano. En caso de manipulación de información confidencial estará incurriendo en la violación a la Ley 1581 de 2012 literal H, donde se enuncia que "Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento" (Pública, 2012)

En caso de la manipulación incorrecta de información por empleados o terceros, conllevará a acciones penales, los implicados en esta situación serán notificados oportunamente ante las autoridades competentes.

6.2 Aplicación de controles Anexo A ISO/IEC 27001

La aplicación de los controles del anexo A, presentes en la norma ISO/IEC 27001 se ejecutan de dos maneras:

- Por vulnerabilidades detectadas: Cada vulnerabilidad detectada en la revisión del estado de las dependencias adscritas a la secretaría de gobierno tendrán su control o sus controles correspondientes para mejorar el nivel y aportar de manera individual y significativamente al mejoramiento del sistema de gestión y por ende a la seguridad de los activos de información.

- De manera generalizada: Dominios que no fueron aplicados en las vulnerabilidades pero que son considerados de vital importancia para las dependencias; son esos dominios que se ajustan a los objetivos iniciales planteados por la secretaría de gobierno.

Capítulo 7

7 PLAN DE MEJORA CONTINUA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

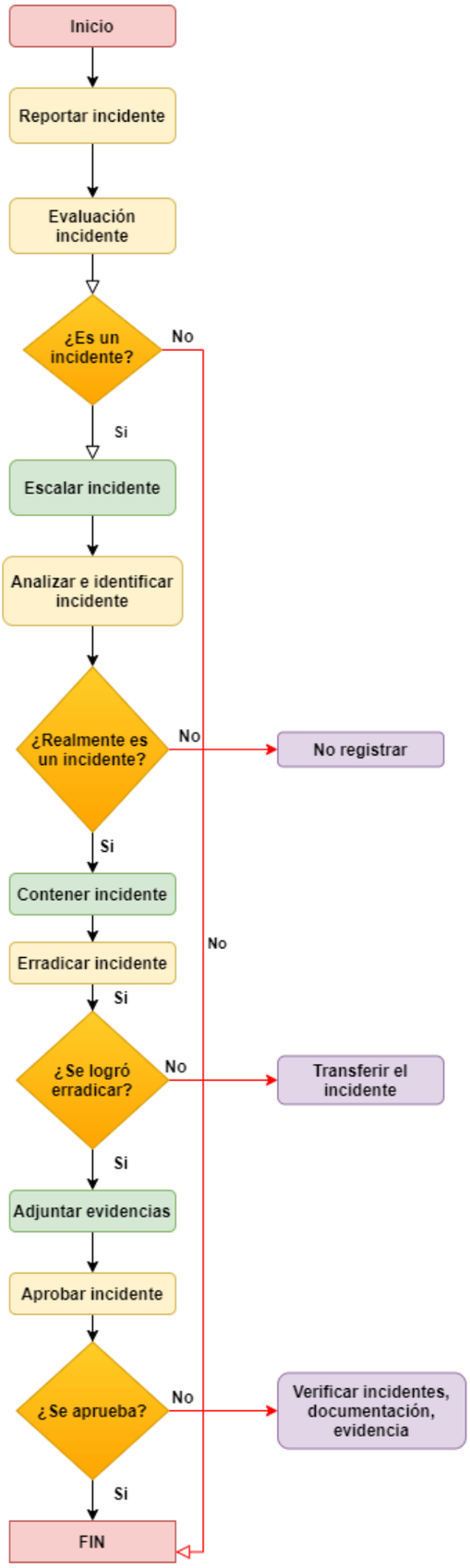
7.1 Procedimiento de revisión de incidentes de seguridad de la información. 62
7.2 Verificación de robustez del sistema de gestión 70
7.3 Suficiencia del SGSI 70

7.1 Procedimiento de revisión de incidentes de seguridad de la información.

El sistema de gestión de seguridad de la información tiene una característica muy particular, y es que se caracteriza por ser cíclico; es por eso que se debe mantener en revisión de forma constante por la secretaría de gobierno. El objetivo del plan de mejora continua del sistema de gestión es uno en común: preservar la confidencialidad, disponibilidad e integridad de los activos de información de la organización, o dependencia donde se implemente. Una vez se mejoren los controles deberán ser puestas en conocimiento a todos los empleados.

Los empleados juegan un papel muy importante en la etapa de revisión de incidentes porque son ellos quienes los registran de acuerdo a las vulnerabilidades detectadas por ellos mismos durante el desarrollo de sus actividades. Para la correcta detección de incidentes deberán seguir cada uno de los pasos establecidos en el diagrama de flujo de la Figura 7.1.

Figura 7.1 Diagrama de flujo: detección de incidentes



Fuente: Gestión incidentes de seguridad Mintic

7.1.1 Interpretación del diagrama de flujo

7.1.1.1 Reportes de incidentes de seguridad de la información

Se debe reportar cualquier información que atente contra la disponibilidad, integridad y confidencialidad de los activos. Son responsables todos los empleados dentro de la secretaría de gobierno de manifestar el incidente en el momento en que se presente, o se sospeche la ocurrencia del evento. En la Figura 7.2 se observa de manera clara esta primera etapa.

Figura 7.2 Etapa inicial el diagrama de flujo

7.1.1.2 Evaluación de los incidentes de seguridad

En esta etapa, se realiza una evaluación para determinar si corresponde a un incidente de seguridad según la lista establecida a continuación:

- Daño o pérdida de información
- Cambios en la información sin autorización
- Acceso no interesado a información privilegiada o equipos ajenos
- Suplantación de identidad.
- Extravío de un activo
- Incumplimiento del plan de tratamiento de riesgos por parte de los empleados adscritos a la secretaría de gobierno o por terceros
- Fallas en la infraestructura que afecta la integridad de los archivos, o la integridad humana

En caso de que el incidente se encuentre clasificado dentro de algún elemento de la lista será clasificado como incidente y se continuará con la sección

de contención. De lo contrario, la gestión de incidente finaliza y se determinará como un evento de falso positivo. La etapa descrita se encuentra en la Figura 7.1, y de manera más clara en la Figura 7.3.

Figura 7.3 Segunda etapa del diagrama de flujo

7.1.1.3 Escalar incidente

Es la etapa en la que el empleado recurre a ayuda profesional para avanzar a la siguiente fase; por lo general el personal de sistemas es el encargado de esta etapa para el posterior análisis del evento. En la Figura 7.4 se observa de manera más clara el bloque descrito.

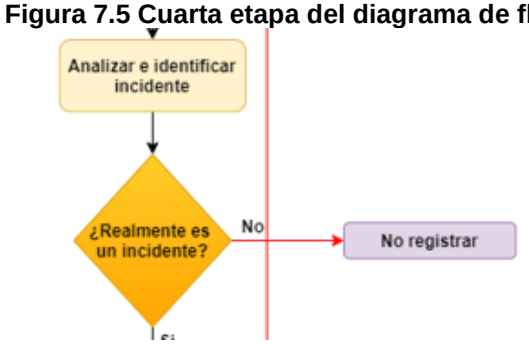
Figura 7.4 Tercera etapa diagrama de flujo

7.1.1.4 Análisis, identificación y revisión del incidente detectado por el empleado

En esta etapa (ver Figura 7.5) el incidente se analiza y se clasifica, con el objetivo de identificar las causas que originaron el incidente dependiendo la información que ha sido afectada y su respectiva ubicación. Si es realmente se determina por el personal de sistemas que se trata de un incidente, se procede con

la siguiente fase que es donde se realizarán acciones correctivas para preservar la información. De lo contrario, el presunto incidente no se registra y finaliza el proceso.

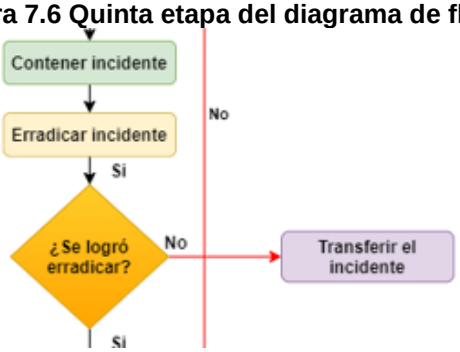
Figura 7.5 Cuarta etapa del diagrama de flujo



7.1.1.5 Contención, erradicación y del incidente detectado

En esta etapa, la cual está especificada en la Figura 7.6 es llamada "**fase correctiva**"**,** debido a que el personal encargado realizará acciones correctivas de cada incidente registrado por los empleados. En cuanto a la **contención** se realizarán todas las tareas necesarias con el fin de minimizar el impacto del evento dentro de la organización y posteriormente erradicar la causa raíz detectada. Si el incidente se logró erradicar satisfactoriamente se procede a la siguiente etapa, aunque en muchas ocasiones según la severidad del incidente éstos no pueden ser solucionados de inmediato, en ese caso se deberán transferir a otras unidades especializadas en la erradicación de riesgos de seguridad de la información y así realizar todas las tareas que sean necesarias con el fin de dar una solución.

Figura 7.6 Quinta etapa del diagrama de flujo



7.1.1.10 Adjuntar evidencia

Esta etapa (ver Figura 7.7) se realiza una vez está solucionado el incidente, y aquí es donde se organizarán todas las evidencias recopiladas a lo largo de todo el proceso con el objetivo de determinar el origen del incidente y los posibles responsables. A su vez, se documentarán las lecciones aprendidas por el personal que ha detectado el incidente, y así saber actuar ante situaciones parecidas que se presenten en futuras ocasiones.

Luego de haber adjuntado toda la evidencia y las lecciones aprendidas por el personal, se continúa con el proceso, avanzando hasta la última sección en donde se revisarán todos los datos recolectados y se aprobará la respuesta al incidente.

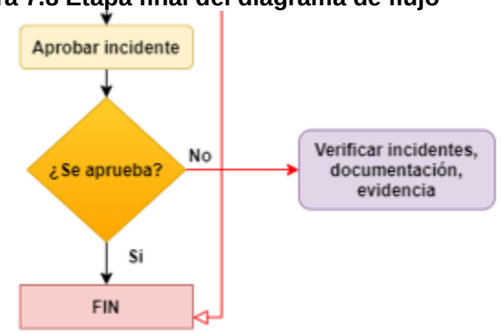
Figura 7.7 Sexta etapa diagrama de flujo

7.1.1.11 Aprobación del incidente

En esta etapa (ver Figura 7.8) el jefe de sistemas revisa todo el proceso realizado anteriormente con el objetivo de aprobar el incidente, en caso de este no ser aprobado se deberá revisar la documentación, lecciones aprendidas y los procedimientos empleados para la eliminación del incidente de seguridad.

Una vez aprobado, la información obtenida en el diagrama de flujo se recopilará en un formato de gestión de incidentes, el cual se observa en la Tabla 7.1

Figura 7.8 Etapa final del diagrama de flujo



A continuación, se muestra el **Encabezado del Formato de control de incidentes de seguridad de la información.** Durante la ejecución del proyecto no fueron detectados incidentes de seguridad, por lo tanto, en el **Anexo 2: Producto tipo** se muestra un ejemplo de cómo llenar el formato de control.

Tabla 7.1 Encabezado del Formato de control de incidentes de seguridad de la información

N° Incidente	Estado	Prioridad	Incidencia	Área	Descripción	Fecha de detección	Detectado por	Asignado a	Adjunta evidencias	Aprobado	Fecha de aprobación de incidente.

Fuente: Propia

Convenciones de la Tabla 7.1:

- **N° incidente:** En esta columna irá el consecutivo de los incidentes detectados, Inicia desde 1.
- **Estado:** Indica la situación actual del incidente, este puede ser abierto o resuelto según sea el caso
- **Prioridad:** Se le atribuye prioridad a cada incidente según el impacto que tenga sobre el correcto desarrollo de las actividades en la entidad y la criticidad de los activos de información involucrados. El estado de prioridad puede ser **Bajo, medio, alto, urgente.**
- **Incidencia:** Se describen las causas provocadas por el incidente de seguridad.
- **Área:** Dependencia u oficina en donde se presenta el incidente
- **Descripción:** Se especifican de manera detallada la incidencia.
- **Fecha de detección:** Fecha en la que se ha detectado el incidente por primera vez.
- **Detectado por:** Persona o empleado que ha detectado el incidente
- **Asignado a:** funcionario de la oficina de sistemas encargado de solucionar el incidente de seguridad
- **Adjunta evidencias:** Fase 6 del diagrama de flujo, corresponde a los soportes entregados durante la investigación y solución del riesgo.
- **Aprobado:** Aval del jefe de sistema después de la revisión de soportes y documentos recolectados en la solución del incidente.
- **Fecha de aprobación de incidente:** Fecha en la que el jefe de sistemas aprobó el incidente registrado.

7.2 Verificación de robustez del sistema de gestión

La robustez del sistema de gestión hace relación al grado de madurez en el que se encuentra el SGSI, y se mide según el porcentaje de implementación de los controles establecidos durante la declaración de aplicabilidad, la rigidez de cada uno de los controles y las competencias adoptadas por los empleados durante todo el proceso de establecimiento de la norma dentro de todas las dependencias adscritas a la secretaría de gobierno. Para la verificación se establecerán fechas en las que el personal encargado de la implementación revisará cada uno de los controles y políticas establecidas, con el objetivo de identificar nuevas brechas, vulnerabilidades y así aumentar la calidad del proceso.

Las competencias que adquieran las personas para actuar frente a incidentes de seguridad juegan un papel muy importante en la consolidación del sistema de gestión, es por eso que se brindarán capacitaciones de manera periódica a todos los empleados orientadas en el descubrimiento de nuevas tendencias y métodos cada vez más efectivos para garantizar a toda costa la disponibilidad, integridad y confidencialidad de los activos de información.

7.3 Suficiencia del SGSI

Aunque la Secretaría de gobierno se encontraba inicialmente en un nivel bajo de madurez, se observa un avance significativo en varios de los dominios que corresponden al 80% de los controles contenidos en el anexo A; esto sucede debido a que gran parte de los controles para la seguridad de la información se encontraban en estado inexistente y ya al día de hoy se encuentran algunos en estado inicial, otros en estado repetible y son de total conocimiento por parte de los empleados y cuentan con la aprobación de la alta dirección.

En cuanto a la evaluación del sistema de Gestión se adaptó la Herramienta de evaluación del programa de seguridad de la información ISO27k que hace parte del **kit de herramientas de la ISO27k.** La herramienta de evaluación mide el nivel

de madurez del SGSI en cualquier organización, consta de 101 preguntas y el tiempo que se tardó en completar es de 5 horas; para calificar la madurez se emplea una escala de 0 a 5, siendo 5 el nivel más alto de madurez.

7.3.1 Niveles de escala de madurez

- **No se ha realizado (0):** No existen controles ni planes de seguridad, es decir, se considera inexistente
- **Realizado informalmente (1):** Existe un acuerdo general dentro de la organización de que las acciones deben ser realizadas, y se ejecutan cuando son necesarios, pero sin adoptarlas de manera formal.
- **Planificado (2):** Los requisitos básicos se planifican y son repetitivos
- **Bien definido (3):** Además de estar planificados, supervisados y repetitivos los procesos, en este nivel son más maduros, ya que están documentados, aprobados y se aplican a nivel general
- **Controlado cuantitativamente (4):** El proceso se mide y se verifica
- **Mejora continua (5):** La principal diferencia con los procesos controlados cuantitativamente, es que estos procesos son revisados y actualizados con regularidad por el personal encargado de la gestión del SGSI.
- **No aplicable:** El proceso no es tenido en cuenta por la organización.

Si se observa detalladamente la escala de madurez, se relaciona de manera directa con los estados aplicados en la declaración de aplicabilidad. En Anexos se encuentra la herramienta de Calificación de madurez del SGSI orientado a la alcaldía municipal de Villanueva la Guajira. La calificación de madurez obtenida es de 3.26 y el estado es **bien definido.**

Conclusiones

De acuerdo a las encuestas realizadas inicialmente, se concluye que el 69% de los empleados no contaban con conocimiento básico de equipos de cómputo, así como se notaron falencias al momento de almacenar información y tener en cuenta medidas de seguridad, lo cual solo aumentaba más la probabilidad de ocurrencia de incidentes. Con las actividades de socialización y concienciación se logró aumentar los conocimientos de cada uno de ellos respecto a las temáticas trabajadas en el diagnóstico.

En la declaración de aplicabilidad el porcentaje de controles inexistentes era del 33%, cifra que se redujo al 0% gracias a la creación e implementación de nuevas políticas dentro de las oficinas adscritas a la secretaría de Gobierno.

El plan de tratamiento de riesgos y las políticas instauradas en cada control establecieron una base importante para el proceso de mejora continua del sistema de gestión; allí se identificaron las amenazas y vulnerabilidades que pueden sufrir cada activo, estimando la magnitud del riesgo según la criticidad de la información y los considerados prioritarios por la alta dirección. Además, se implementa una tabla donde se relaciona la probabilidad de ocurrencia y el impacto que tendría cada evento donde pueda perjudicarse la confidencialidad, integridad y disponibilidad de la información en la secretaría de gobierno, manifestando de manera implícita la importancia de seguir las indicaciones y cumplir las políticas establecidas de manera correcta por parte del personal que allí labore.

Para disminuir los riesgos relacionados con la seguridad de la información en la alcaldía municipal se inicia con la identificación de los riesgos que comprometen la seguridad, seguido de la creación de políticas para prevención de riesgos, monitorearlos constantemente y por último pero no menos importante, concientizar

a los empleados de que la seguridad de la información es una problemática que no solo afecta a la entidad sino a ellos mismos debido a que los perjuicios que conlleva omitirlos son muy perjudiciales. Todo esto en respuesta a la pregunta problematizadora planteada en el Planteamiento del Problema

En la implementación del sistema de gestión es importante el liderazgo y el compromiso aportado por la alta dirección, que en este caso estuvo a cargo del secretario de gobierno, quien se encargó de verificar que las políticas diseñadas se ejecuten y se cumplan de manera correcta por parte de los empleados en la búsqueda de la consecución de los objetivos planteados. Adicionalmente gracias a la alta dirección los procesos se integran a las actividades de la secretaría y sus dependencias de forma satisfactoria; por lo cual se llega a la conclusión de que, un SGSI sin apoyo de la alta dirección no lograría buenos resultados.

El presente proyecto establece las bases fundamentales para la implementación del SGSI en la secretaría de gobierno de la alcaldía municipal de Villanueva la Guajira, pero siempre estará sujeto al proceso de mejora continua considerando en una próxima aplicación aumentar las áreas o dependencias que se acojan al sistema.

La calificación final del SGSI en la Secretaría de Gobierno fue de 3.26, lo cual significa que la madurez del sistema se ubica en nivel **bien definido.** Resultado considerado muy significativo para el sistema de gestión, nada comparable con la puntuación inicial (0); la secretaría debe seguir trabajando en implementación de políticas y seguimiento riguroso a los controles donde la calificación es baja, para alcanzar el nivel de madurez deseado que es de 4.52.

El aporte realizado por el estudiante Carlos Sarmiento a la alcaldía Municipal de Villanueva La Guajira a través de la implantación del Sistema de Gestión de Seguridad de la Información SGSI, se traduce no solo en la aplicación del conocimiento adquirido a través de su formación profesional, además, se integra en

un ahorro económico para la alcaldía, aproximado, entre 8 y 10 millones de pesos, este valor corresponde al costo en el mercado, de los servicios prestados por empresas consultores que ofrecen el servicios de implementar la norma a la medida de sus clientes, para este caso se tomó como referencia, la empresa internacional Advisera (ADVISERA, 2021), donde la documentación tiene un coste inicial de 3.486.689 en pesos colombianos (US $897) y adicional a eso las auditorias y mantenimiento del sistema para la mejora continua es de 5.497.320 pesos (US $1414,39), de igual manera la empresa ofrece una herramienta de verificación de cumplimiento de la norma, que tiene un costo mensual, de 773254 pesos (US $199); a nivel local, empresas como bureau veritas, 2secure, capitalis latam también ofrecen el servicio de implementación de la norma, con la particularidad que lo hacen según los procesos que se deseen certificar; con un total aproximado de 9.757.533 pesos

RECOMENDACIONES

- La implementación del sistema de gestión de seguridad de la información SGSI es un proceso que toma tiempo, recursos económicos y lo más importante **compromiso**, sin embargo, beneficia de manera significativa el crecimiento de las empresas si su gestión se realiza de forma correcta. Es por eso que se recomienda seguir implementando para la solidez del sistema mediante ciclos de mejora continua.
- Debido a las vulnerabilidades y riesgos identificadas dentro de la secretaría de gobierno, se recomienda ampliar la implementación del sistema de gestión a las demás oficinas de la alcaldía municipal para tratar los riesgos que comprometan los activos de la información de las demás dependencias, y que la secretaría de gobierno sea tomada como modelo ante la planificación del sistema de gestión de forma institucional.

Bibliografía

ADVISERA, 2021. *27001 Academy.* [En línea]
Available at: https://advisera.com/27001academy/pricing/

Congreso de Colombia, 2009. *Ley 1341 de 2009.* [En línea]
Available at: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913
[Último acceso: 2021].

Congreso de la república, 2020. *Asuntos legales.* [En línea]
Available at: https://www.asuntoslegales.com.co/analisis/mariana-gutierrez-duque-2880351/el-derecho-de-propiedad-intelectual-en-colombia-le-otorga-a-su-titular-derechos-en-otros-paises-3001834
[Último acceso: Noviembre 2021].

Consejo Nacional de política económica y social CONPES, 2016. *CONPES*. [En línea]
Available at: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf
[Último acceso: 4 Noviembre 2021].

Función pública, 2012. *Ley 1581 de 2012.* [En línea]
Available at: https://www.mintic.gov.co/arquitecturati/630/articles-9011_documento.pdf
[Último acceso: Noviembre 2021].

Función Pública, 2014. *Ley 1712 de 2014.* [En línea]
Available at:

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882
[Último acceso: Noviembre 2021].

ICONTEC, 2006. *Norma Técnica Colombiana NTC-ISO/IEC Colombiana 27001.* [En línea]
Available at: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma. NTC-ISO-IEC 27001.pdf
[Último acceso: Septiembre 2021].

Instituto nacional de ciberseguridad , 2017. *INCIBE.* [En línea]
Available at: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
[Último acceso: Noviembre 2021].

ISO, s.f. *ISO27K Toolkit.* [En línea]
Available at: https://www.iso27001security.com/html/toolkit.html
[Último acceso: Septiembre 2021].

Javier Ruiz Spohr, A. L. N., 2005. *SGSI.* [En línea]
Available at: https://www.iso27000.es/sgsi.html
[Último acceso: Septiembre 2021].

MinCiencias, 2021. *Minciencias.gov.co.* [En línea]
Available at: https://minciencias.gov.co/sites/default/files/ckeditor_files/D103PR03%20Gestión%20de%20Incidente%20de%20seguridad%20de%20la%20Información%20V01.pdf
[Último acceso: Noviembre 2021].

Ministerio de Tecnologías de la Información y las Comunicaciones, 2016. *Modelo de Seguridad y Privacidad de La Información - Guía de Mejora Continua.* [En línea]
Available at:

https://www.mintic.gov.co/gestionti/615/articles5482_Modelo_de_Seguridad_Privacidad.pdf%0Ahttps://www.mintic.gov.co/gestionti/61
[Último acceso: Noviembre 2021].

MINTIC, 2018. *Resolución 1443 de 2018.* [En línea] Available at: https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_1443_2018.htm
[Último acceso: Noviembre 2021].

MINTIC, 2020. *Resolución mintic 1519 de 2020.* [En línea] Available at: https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_1519_2020.htm
[Último acceso: Noviembre 2021].

MINTIC, s.f. *Gobierno Digital.* [En línea] Available at: https://gobiernodigital.mintic.gov.co/portal/
[Último acceso: 2021].

Organization International Standard, 2018. *INTERNATIONAL STANDARD ISO / IEC 27001 — Information security management systems —.* [En línea] Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
[Último acceso: Septiembre 2021].

Organization, I. S., 2004. *ISO/IEC TR 18044:2004, Information Technology. Security Techniques. Information.* s.l.:s.n.

Pública, F., 2012. *Ley estatutaria 1581 de 2012.* [En línea] Available at: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
[Último acceso: 2021].

SUIN, 2014. *Ley 1712 de 2014.* [En línea] Available at: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1687091 [Último acceso: Noviembre 2021].

SUIN, 2015. *Decreto 103 de 105.* [En línea] Available at: http://suin.gov.co/viewDocument.asp?ruta=Decretos/30019726 [Último acceso: Noviembre 2021].

Sullivan, P., 2016. *ComputerWeekly.es.* [En línea] Available at: https://www.computerweekly.com/es/consejo/Gestion-de-riesgos-de-seguridad-de-la-informacion-Comprension-de-los-componentes [Último acceso: 4 Noviembre 2021].

TECON, 2018. *Blog: Simplificando la tecnología.* [En línea] Available at: https://www.tecon.es/la-seguridad-de-la-informacion/ [Último acceso: Septiembre 2021].

Anexos

Ficha técnica perteneciente al Análisis. Del capítulo 4.1.1

Anexo 1 Encuesta de caracterización

1. ¿Sabe usted que es un activo de información?
   a. Si
   b. No
2. ¿Conoce usted que es seguridad de la información?
   a. Si
   b. No
3. En el trabajo, ¿utiliza su computador personal o uno institucional?
   a. Personal
   b. Institucional
   c. No dispongo de un equipo
4. En caso de utilizar un computador institucional, ¿Dispone usted de una cuenta de invitado?
   a. Si
   b. No
5. ¿Emplea contraseñas para el inicio de sesión?
   a. Si
   b. No
6. ¿Comparte su contraseña con otras personas de la oficina o ajenas a ellas?
   a. Si
   b. No
7. ¿Permite que su equipo lo utilicen otras personas aparte de usted?
   a. Si
   b. No
8. ¿Organizas los archivos digitales por carpetas según su clasificación?
   a. Si
   b. No
9. ¿Proteges los archivos de información digital con algún cifrado o contraseñas?
   a. Si
   b. No

10. ¿Organizas los documentos físicos por folios, carpetas o por bloques según su clasificación?
   a. Si
   b. No

11. ¿Tiene algún estante para guardar los documentos físicos?
   a. Si
   b. No

12. ¿El estante tiene cerradura/candado en buen estado?
   a. Si
   b. No

13. ¿Su computador cuenta con antivirus licenciado?
   a. Si
   b. No

14. ¿Sabe que es un virus informático?
   a. Si
   b. No

15. ¿Tiene conocimiento sobre cómo actuar en caso de detectar un virus?
   a. Si
   b. No

16. ¿Realiza copias de seguridad de su información de manera periódica? De ser positiva su respuesta, favor indicar cada cuánto lo realiza
   a. Si
   b. No

_____

17. ¿Introduce memorias, discos duros, o cualquier otro dispositivo extraíble para el intercambio de información?
   a. Si
   b. No

18. ¿Tiene conocimiento acerca de la existencia de políticas de gestión de riesgos de la información?
   a. Si
   b. No

19. ¿Tiene conocimiento acerca de políticas de tratamiento de información confidencial?
   a. Si
   b. No

20. ¿Tiene conocimiento acerca de políticas de ahorro energético?
   a. Si
   b. No

21. ¿Sabe usted si en la entidad existen políticas de seguridad de la información?
   a. Si
   b. No

22. ¿Guarda información personal (como fotos, videos, música) dentro de su equipo institucional?
   a. Si
   b. No

23. ¿Su oficina cuenta con un plan de contingencia de riesgos o desastres (Inundaciones, incendio, alteraciones)
   a. Si
   b. No

24. ¿Las puertas y ventanas de su dependencia se encuentran en buen estado?
   a. Si
   b. No
   c. Casi todas

25. ¿Le realiza mantenimiento preventivo a su equipo? De ser positivo su respuesta, por favor indique cada cuanto tiempo
   a. Si
   b. No

_____

26. ¿Sabe usted qué es un delito informático?
   a. Si
   b. No

27. ¿Sabe que es Phishing?
   a. Si
   b. No

28. ¿Ha recibido correos no deseados, sospechosos o fraudulentos, donde le ofrecen algún tipo de recompensa o premio?
   a. Si
   b. No

29. ¿Ha recibido correos donde suplanten la identidad de algún funcionario o familiar?
   a. Si
   b. No

30. ¿Tiene libertad para instalar aplicaciones, programas o cualquier tipo de software en su equipo de trabajo?
   a. Si

b. No

Producto tipo: Gestión de incidentes de seguridad de la información.

Anexo 2 Producto tipo incidentes de seguridad

N° Incidente	Estado	Prioridad	Incidencia	Área	Descripción	Fecha de detección	Detectado por	Asignado a	Adjunta evidencias	Aprobado	Fecha de aprobación de incidente.
1	Resuelto	Inmediata	Acceso no autorizado	Comisaría De familia	Abuso de información privilegiada y actos no autorizados	17/11/2021	Carla Meza	Carlos Sarmiento	Si	Si	20/11/2021
2	Abierto	Alta	Corrupción de la información	Jurídica	Ataque interno de un funcionario sin identificar	19/11/2021	Ronald Liñan	Jacen Sánchez	No	No	-

Herramienta para determinar madurez del SGSI, perteneciente al capítulo 7.3.1

Fuente: Adaptado de www.iso27001security.com

Anexo 3 Calificación de madurez del SGSI

ID No.	Preguntas	Nivel de Madurez Actual	Puntuación Actual	Nivel de Madurez Deseado	Puntuación Deseada
	Gestión de riesgos (ISO 27005:2011)		**3,67**		**5,00**
1	¿Tiene la organización una persona o grupo que tenga la función y la responsabilidad de un proceso continuo de evaluación de la probabilidad de que las amenazas conocidas exploten las vulnerabilidades y el consiguiente impacto en los activos valiosos? La gestión de riesgos también asigna prioridades relativas para los planes de mitigación y su aplicación.	Yes	5	Yes	5
2	¿Dispone la organización de un proceso para identificar y evaluar los riesgos internos y externos que sean razonablemente previsibles para la seguridad, la confidencialidad y/o la integridad de cualquier registro electrónico, en papel o de otro tipo que contenga información sensible?	Bien Definido	3	Mejora Continua	5

3	¿Realiza la organización evaluaciones de riesgo rutinarias para identificar los objetivos clave que deben ser apoyados por el programa de seguridad de la información?	Bien Definido	3	Mejora Continua	5
	Políticas de seguridad de la información (ISO 5)		**4,00**		**4,67**
4	¿Tiene la organización una política de seguridad de la información que haya sido aprobada por la dirección?	Bien Definido	3	Cuantitativamente controlado	4
5	¿Se ha publicado la política de seguridad y se ha comunicado a todas las partes interesadas?	Mejora Continua	5	Mejora Continua	5
6	¿Revisa la organización la política de seguridad a intervalos definidos para abarcar los cambios significativos y supervisar su cumplimiento?	Cuantitativamente controlado	4	Mejora Continua	5
	Organización de la Seguridad de la Información (ISO 6)		**3,50**		**4,33**
7	¿Tiene la función de seguridad de la información la autoridad necesaria para gestionar y garantizar el cumplimiento del programa de seguridad de la información?	Mejora Continua	5	Mejora Continua	5

8	¿Cuenta la organización con una persona con responsabilidad y autoridad en materia de seguridad de la información en toda la empresa, incluida en la descripción de su puesto de trabajo, o equivalente?	Bien Definido	3	Bien Definido	3
9	¿Está claramente asignada la responsabilidad de todas las áreas de la arquitectura de seguridad de la información, el cumplimiento, los procesos y las auditorías?	No Aplicable		No Aplicable	
10	¿Existe un proceso formal para que la persona responsable de la seguridad de la información evalúe y apruebe el hardware, el software y los servicios adecuados, asegurándose de que siguen las políticas y los requisitos de seguridad?	Cuantitativamente controlado	4	Mejora Continua	5
11	¿Mantiene la organización relaciones con las autoridades locales?	Mejora Continua	5	Mejora Continua	5
12	¿Participa la organización en grupos, asociaciones y organismos de seguridad locales, nacionales o internacionales?	Cuantitativamente controlado	4	Mejora Continua	5
13	¿Tiene la organización revisiones de seguridad independientes realizadas a intervalos planificados o cuando se producen cambios significativos en el entorno?	No se ha realizado	0	Bien Definido	3
	Seguridad de los recursos humanos (ISO 7)		**3,40**		**5,00**

14	¿Todas las personas que interactúan con el sistema de información de la organización reciben formación sobre seguridad de la información?	Mejora Continua	5	Mejora Continua	5
15	¿Realiza la organización una formación especializada basada en las funciones?	Bien Definido	3	Mejora Continua	5
16	¿Los programas de seguridad de la información establecen claramente las responsabilidades, las obligaciones y las consecuencias?	Mejora Continua	5	Mejora Continua	5
17	¿Dispone la organización de un proceso para revocar el acceso al sistema y al edificio y devolver los activos asignados?	Planeado	2	Mejora Continua	5
18	¿Dispone la organización de un proceso para revocar el acceso al sistema cuando hay un cambio de puesto o cuando cambian las responsabilidades?	Planeado	2	Mejora Continua	5
	Gestión de activos (ISO 8)		**4,50**		**5,00**
19	¿Ha identificado la organización los activos de información críticos y las funciones que dependen de ellos?	Mejora Continua	5	Mejora Continua	5
20	¿La organización clasifica la información para indicar los niveles adecuados de seguridad de la información?	Cuantitativamente controlado	4	Mejora Continua	5
	Control de Acceso (ISO 9)		**3,09**		**4,45**

21	¿Tiene la organización una política de control de acceso para autorizar y revocar los derechos de acceso a los sistemas de información?	Mejora Continua	5	Mejora Continua	5
22	¿Dispone la organización de un proceso para conceder y revocar el acceso adecuado a los usuarios?	Planeado	2	Cuantitativamente controlado	4
23	¿Dispone la organización de un programa de gestión de contraseñas que siga las normas de seguridad vigentes?	Bien Definido	3	Cuantitativamente controlado	4
24	¿Dispone la organización de procedimientos para revisar periódicamente el acceso de los usuarios a fin de garantizar que sólo se apliquen los privilegios necesarios?	Realizado Informalmente	1	Cuantitativamente controlado	4
25	¿Emplea la organización medidas específicas para asegurar los servicios de acceso remoto?	No Aplicable		No Aplicable	
26	¿Emplea la organización tecnologías para bloquear o restringir que la información sensible no cifrada viaje a través de redes no fiables?	No se ha realizado	0	Cuantitativamente controlado	4
27	¿Dispone la organización de mecanismos para gestionar las identidades digitales (cuentas, claves, tokens) a lo largo de su ciclo de vida, desde el registro hasta la finalización?	No Aplicable		No Aplicable	
28	¿Existe una política para evitar que se compartan las contraseñas?	Mejora Continua	5	Mejora Continua	5
29	¿Prohíbe la organización el uso de cuentas genéricas con acceso privilegiado a los sistemas?	Bien Definido	3	Cuantitativamente controlado	4

30	¿Dispone la organización de un sistema de autenticación que aplique niveles más altos de autenticación para proteger los recursos con mayores niveles de sensibilidad?	Planeado	2	Cuantitativamente controlado	4
31	¿Dispone la organización de un sistema de autorización que imponga el límite de los tiempos para bloquearse en caso de fallo en el inicio de la sesión y que se ajuste por defecto a los privilegios mínimos?	No Aplicable		No Aplicable	
32	¿Dispone la organización de normas para aislar los datos sensibles y procedimientos y tecnologías para protegerlos del acceso no autorizado y la manipulación?	Mejora Continua	5	Mejora Continua	5
33	¿Tiene la organización una guía de uso establecida para los dispositivos informáticos móviles (independientemente de la propiedad) que almacenan, procesan o transmiten datos de la organización?	Mejora Continua	5	Mejora Continua	5
34	¿Exige la organización el cifrado de los dispositivos informáticos móviles (es decir, ordenadores portátiles, tabletas, etc.)?	Bien Definido	3	Mejora Continua	5
35	¿Dispone la organización de una política de teletrabajo (trabajo a distancia) que considere los requisitos de acceso y seguridad multi-factor para el dispositivo final que se utiliza?	No Aplicable		No Aplicable	
	Criptografía (ISO 10)		**0,00**		**3,67**

36	¿Utiliza la organización métodos de encriptación apropiados o comprobados para proteger los datos sensibles en tránsito?	No se ha realizado	0	Bien Definido	3
37	¿Indican las políticas cuándo debe utilizarse el cifrado (por ejemplo, en reposo, en tránsito, con datos sensibles o confidenciales, etc.)?	No Aplicable		Bien Definido	3
38	¿Están los estándares de gestión de claves documentados y se utilizan?	No Aplicable		Mejora Continua	5
	Seguridad física y medioambiental (ISO 11)		**3,00**		**4,60**
39	¿Incluyen los centros de datos de la organización controles para garantizar que sólo se permite el acceso físico a las partes autorizadas?	No Aplicable		No Aplicable	
40	¿Dispone la organización de medidas de prevención para proteger hardware crítico y el cableado de las amenazas naturales y provocadas por el hombre?	Bien Definido	3	Mejora Continua	5

41	¿Dispone la organización de un proceso para la emisión de llaves, códigos y/o tarjetas que requieran una autorización adecuada y la comprobación de antecedentes para el acceso a estas instalaciones sensibles?	Realizado Informalmente	1	Bien Definido	3
42	¿Sigue la organización las directrices recomendadas por el proveedor para el mantenimiento de los equipos?	Bien Definido	3	Mejora Continua	5
43	¿Dispone la organización de un proceso de desinfección de medios que se aplica a los equipos antes de su eliminación, reutilización o liberación?	Mejora Continua	5	Mejora Continua	5
44	¿Existen procesos para detectar la retirada no autorizada de equipos, información o software?	Bien Definido	3	Mejora Continua	5
	Seguridad de las operaciones (ISO 12)		**2,82**		**4,38**
45	¿Mantiene la organización normas de configuración de seguridad para los sistemas de información y las aplicaciones?	Bien Definido	3	Mejora Continua	5

46	¿Se comprueban, autorizan y notifican los cambios en los sistemas de información?	Bien Definido	3	Mejora Continua	5
47	¿Están las funciones suficientemente separadas para garantizar la detección de modificaciones no intencionadas o no autorizadas de la información?	Mejora Continua	5	Mejora Continua	5
48	¿Están los sistemas de producción separados de otras etapas del ciclo de vida del desarrollo?	No Aplicable		Mejora Continua	5
49	¿Dispone la organización de procesos para supervisar la utilización de los recursos clave del sistema y para mitigar el riesgo de que el sistema esté fuera de servicio?	No Aplicable		No Aplicable	

50	¿Se utilizan métodos para detectar, poner en cuarentena y erradicar los códigos maliciosos conocidos en los sistemas de información, incluidas las estaciones de trabajo, los servidores y los dispositivos informáticos móviles?	No Aplicable		No Aplicable	
51	¿Se utilizan métodos para detectar y erradicar el código malicioso conocido que se transporta por correo electrónico, la web o los medios extraíbles?	Bien Definido	3	Mejora Continua	5
52	¿La frecuencia del proceso de copia de seguridad de los datos es coherente con los requisitos de disponibilidad de la organización?	Mejora Continua	5	Mejora Continua	5
53	¿Dispone la organización de un proceso de comprobación de la reputación, como el software antivirus actual, el cortafuegos activado, el nivel de parches del sistema operativo, etc., de los dispositivos cuando se conectan a su red?	Realizado Informalmente	1	Bien Definido	3

54	¿Dispone la organización de una arquitectura de red segmentada para proporcionar diferentes niveles de seguridad en función de la clasificación de la información?	No se ha realizado	0	Mejora Continua	5
55	¿Los servidores accesibles por Internet están protegidos por más de una capa de seguridad (cortafuegos, IDS de red, IDS de host, IDS de aplicación)?	No Aplicable		No Aplicable	
56	¿Existen controles para proteger, rastrear e informar sobre el estado de los medios que han sido retirados de los sitios seguros de la organización?	Realizado Informalmente	1	Bien Definido	3
57	¿Dispone la organización de un proceso para garantizar que los datos relacionados con el comercio electrónico (e-commerce) que atraviesan las redes públicas están protegidos de actividades fraudulentas, divulgación no autorizada o modificación?	No Aplicable		No Aplicable	

58	¿Se registran automáticamente las actividades relacionadas con la seguridad, como los cambios de configuración del hardware, los cambios de configuración del software, los intentos de acceso y las asignaciones de autorizaciones y privilegios?	No Aplicable		No Aplicable	
59	¿Dispone la organización de un proceso de supervisión rutinaria de los registros para detectar actividades no autorizadas y anómalas?	Planeado	2	Cuantitativamente controlado	4
60	¿Registra la organización las revisiones del registro (recertificación/ atestación)?	Bien Definido	3	Mejora Continua	5
61	¿Se toman medidas para asegurar los datos de registro para evitar el acceso no autorizado y la manipulación?	Mejora Continua	5	Mejora Continua	5
62	¿Revisa la organización regularmente el acceso administrativo y operativo a los registros de auditoría?	No Aplicable		Planeado	2

63	¿Se utilizan herramientas de supervisión de la integridad de los archivos para alertar al personal de la modificación no autorizada de los archivos críticos del sistema, los archivos de configuración o los archivos de contenido, y para configurar el software para que realice comparaciones de los archivos críticos al menos una vez por semana?	No Aplicable		No Aplicable	
64	¿Dispone la organización de un proceso que garantice la sincronización de los relojes del sistema con una fuente autorizada (por ejemplo, a través de NTP) de forma periódica y proporcional a los riesgos potenciales?	No Aplicable		No Aplicable	
	Seguridad de las comunicaciones (ISO 13)		**3,20**		**4,00**
65	¿Exige la organización el uso de acuerdos de confidencialidad o no divulgación para los empleados y terceros?	Mejora Continua	5	Mejora Continua	5

66	¿Prueba la organización de forma rutinaria sus procedimientos de restauración?	Planeado	2	Cuantitativamente controlado	4
67	¿Supervisa la organización continuamente sus redes alámbricas e inalámbricas para detectar accesos no autorizados?	Bien Definido	3	Bien Definido	3
68	¿Dispone la organización de políticas y procedimientos para proteger el intercambio de información (dentro de la organización y en acuerdos con terceros) contra la interceptación, la copia, la modificación, el desvío y la destrucción?	Mejora Continua	5	Mejora Continua	5
69	¿Garantiza la organización que el acceso de los usuarios al diagnostico y configuración de los puertos está restringido para las personas autorizadas?	Realizado Informalmente	1	Bien Definido	3
70	¿Emplea la organización medidas específicas para prevenir y detectar puntos de acceso fraudulentos para todas sus LAN inalámbricas?	No Aplicable		No Aplicable	

	Adquisición, desarrollo y mantenimiento de sistemas (ISO 14)		**3,33**		**4,67**
71	¿Dispone la organización de un proceso para validar la seguridad de los productos y servicios de software adquiridos?	Planeado	2	Cuantitativamente controlado	4
72	¿Se validan los nuevos sistemas de información o las mejoras de los sistemas de información existentes con respecto a los requisitos de seguridad definidos?	Bien Definido	3	Mejora Continua	5
73	¿Se han establecido normas que aborden prácticas de codificación seguras (por ejemplo, validación de entradas, gestión adecuada de errores, gestión de sesiones, etc.) y que tengan en cuenta las vulnerabilidades de seguridad habituales en las aplicaciones (por ejemplo, CSRF, XSS, inyección de código, etc.)?	No Aplicable		No Aplicable	
74	¿Se incorporan controles de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados?	No Aplicable		No Aplicable	
75	¿Existen procesos para comprobar si la integridad de los mensajes es necesaria?	No Aplicable		No Aplicable	

76	Pueden producirse resultados incorrectos, incluso en sistemas probados. ¿Tiene la organización controles de validación para garantizar que la salida de datos es la esperada	No Aplicable		No Aplicable	
77	¿Establece la organización procedimientos para mantener el código fuente durante el ciclo de vida de desarrollo y mientras está en producción para reducir el riesgo de corrupción del software?	No Aplicable		No Aplicable	
78	¿Aplica la organización las mismas normas de seguridad para los datos sensibles de prueba que se aplican también a los datos sensibles de producción?	No Aplicable		No Aplicable	
79	¿Restringe y controla la organización el acceso a las bibliotecas de código fuente para reducir el riesgo de corrupción?	No Aplicable		No Aplicable	
80	¿Dispone la organización de un proceso de gestión de la configuración que garantice que los cambios en los sistemas críticos obedecen a razones empresariales válidas y han recibido la debida autorización?	No Aplicable		No Aplicable	
81	¿Se realizan revisiones y pruebas para garantizar que los cambios realizados en los sistemas de producción no tengan un impacto adverso en la seguridad o las operaciones?	No Aplicable		No Aplicable	
82	¿Implementa la organización herramientas y procedimientos para controlar y prevenir la pérdida de datos sensibles?	Mejora Continua	5	Mejora Continua	5

83	¿Incluyen los acuerdos contractuales requisitos de seguridad para el desarrollo de software subcontratado?	No Aplicable		No Aplicable	
84	¿Cuenta la organización con una estrategia de gestión de parches y con responsabilidades asignadas para supervisar y responder rápidamente a las publicaciones de parches, boletines de seguridad e informes de vulnerabilidad?	No Aplicable		No Aplicable	
	Relaciones con los proveedores (ISO 15)		**3,67**		**4,33**
85	¿Especifica la organización los requisitos de seguridad en los contratos con entidades externas (terceros) antes de conceder el acceso a los activos de información sensibles de la organización?	Mejora Continua	5	Mejora Continua	5
86	¿Se abordan y corrigen los requisitos antes de conceder el acceso a los datos, activos y sistemas de información?	Mejora Continua	5	Mejora Continua	5
87	¿Los acuerdos para los servicios de sistemas de información externos especifican los requisitos de seguridad adecuados?	No Aplicable		No Aplicable	
88	¿Dispone la organización de un proceso para evaluar que los proveedores de sistemas de información externos cumplen con los requisitos de seguridad adecuados?	No Aplicable		No Aplicable	

89	¿Se supervisa el cumplimiento de los controles de seguridad por parte del proveedor externo de servicios de información?	Realizado Informalmente	1	Bien Definido	3
90	¿Se ejecutan y revisan rutinariamente los acuerdos de servicio del sistema de información externo para garantizar que los requisitos de seguridad están actualizados?	No Aplicable		No Aplicable	
	Gestión de incidentes de seguridad de la información (ISO 16)		**5,00**		**5,00**
91	¿Existen procedimientos de gestión de incidentes para informar y responder a los eventos de seguridad a lo largo del ciclo de vida del incidente, incluyendo la definición de funciones y responsabilidades?	Mejora Continua	5	Mejora Continua	5
92	¿Conoce el personal de respuesta a incidentes los requisitos legales o de cumplimiento que rodean a la recogida de pruebas?	Mejora Continua	5	Mejora Continua	5
	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio (ISO 17)		**1,00**		**5,00**

93	¿Dispone la organización de un plan documentado de continuidad del negocio para la tecnología de la información que se base en un análisis del impacto del negocio, que se pruebe periódicamente y que haya sido revisado y aprobado por el personal superior o el consejo de administración?	Realizado Informalmente	1	Mejora Continua	5
	Cumplimiento (ISO 18)		**3,57**		**4,71**
94	¿Dispone la organización de una política de gestión de archivos o de gobernanza de datos que aborde el ciclo de vida de los documentos de archivo tanto en papel como en formato electrónico en su organización?	Mejora Continua	5	Mejora Continua	5
95	¿Dispone la organización de una política de protección de datos aplicable que cubra la información personal identificable (PII)?	Mejora Continua	5	Mejora Continua	5
96	¿Tiene la organización una normativa de buen uso que defina el uso indebido?	Mejora Continua	5	Mejora Continua	5
97	¿Proporciona la organización orientación a los empleados sobre las leyes de control de las exportaciones de archivos?	Mejora Continua	5	Mejora Continua	5

98	¿Se evalúan periódicamente los procedimientos operativos estándar para comprobar el cumplimiento de las políticas, normas y procedimientos de seguridad de la organización?	Bien Definido	3	Mejora Continua	5
99	¿Realiza la organización pruebas periódicas de vulnerabilidad de la aplicación y de la capa de red o pruebas de penetración contra los sistemas de información críticos?	Planeado	2	Cuantitativamente controlado	4
100	¿Realiza la organización auditorías independientes de los sistemas de información para identificar los puntos fuertes y débiles?	No se ha realizado	0	Cuantitativamente controlado	4
101	¿Están las herramientas de auditoría debidamente separadas de los entornos de los sistemas de desarrollo y operativos para evitar cualquier uso indebido o compromiso?	No Aplicable		No Aplicable	
	Madurez media (porcentaje y niveles)	**Estado Actual**	**3,26**	**Estado deseado**	**4,52**