# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
# AÑO 2019
# FONDO DE VIVIENDA DE INTERÉS SOCIAL Y REFORMA URBANA DISTRITAL- CORVIVIENDA

Dir: Manga 3ª Avenida, Calle 28 #21-62
Email: info@corvivienda.gov.co
wwww.corvivienda.gov.co
Tel: 6445429 - 6445074

# DIRECTIVOS CORVIVIENDA

| | |
|---|---|
| **ÉRICA BARRIOS BLANQUICETH** | Gerente |
| **JOSE UTRIA MONSALVE** | Director Administrativo |
| **MIGUEL RAMÓN MÉNDEZ PAREDES** | Director Técnico |
| **NATACHA GONZALEZ VALLEJO** | Jefe Oficina Asesora de Planeación |
| **ISABEL DIAZ MARTINEZ** | Jefe Oficina Asesora de Jurídica |
| **JAVIER ERNESTO CAMACHO DIAZ** | Jefe Oficina de Control Interno |

_____

**Aprobó: ÉRICA BARRIOS BLANQUICETH** **Gerente**
**Revisó: NATACHA GONZALEZ VALLEJO** **Jefe Oficina Asesora Planeación**
**Elaboró: ISSI TUÑON ARROYO** **Contratista**
**.**

**TABLA DE CONTENIDO**


1. INTRODUCCIÓN ..... 5
2. OBJETIVOS ..... 7
   2.1. OBJETIVO GENERAL ..... 7
   2.2. OBJETIVOS ESPECÍFICOS ..... 7
3. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD ..... 8
   3.1. CICLO DE OPERACIÓN ..... 8
   3.2. ALINEACIÓN NORMA ISO 27001:2013 VS CICLO DE OPERACIÓN ..... 9
   3.3. FASE I: DIAGNÓSTICO ..... 11
   3.4. FASE II: PLANIFICACIÓN ..... 12
   3.5. FASE III: IMPLEMENTACIÓN ..... 14
   3.6. FASE IV: EVALUACIÓN DE DESEMPEÑO ..... 15
   3.7. FASE V: MEJORA CONTINUA ..... 16
4. TÉRMINOS Y REFERENCIAS ..... 17

## ÍNDICE DE FIGURAS

Figura 1. Ciclo de operación Modelo de Seguridad y Privacidad de la Información 8
Figura 2. Norma ISO 27001:2003 alineado al Ciclo de mejora continua ..... 9
Figura 3. Fase de planificación modelo de seguridad ..... 12
Figura 4. Fase de implementación modelo de seguridad ..... 14
Figura 5. Fase Evaluación Desempeño modelo de seguridad ..... 16
Figura 6. Fase Mejora Continua modelo de seguridad..... 16

## ÍNDICE DE TABLAS

Tabla 1. Fases ciclo operación Vs estructura ISO 27001:2013..... 9

# 1. INTRODUCCIÓN

La información se constituye como uno de los activos más valiosos para cualquier entidad u organización, la cual sólo cobra validez cuando está disponible y se utiliza de forma adecuada, integra, oportuna, responsable y segura. Esto implica que las organizaciones cuenten con una adecuada gestión de sus recursos y activos de información, con el fin de asegurar y controlar el debido acceso, tratamiento y uso de la información.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

Toda organización debe ser consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y su supervivencia. Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones. Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, constantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si ésta es de carácter organizacional o personal, o de tipo pública o privada.

En la medida que las organizaciones tenga una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad tanto de la información de la organización como los datos de carácter personal de sus empleados, usuarios y partes interesadas. Es indispensable que las organizaciones realicen una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos que pueden afectar su seguridad, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

Debido a los múltiples riesgos y amenazas que hoy en día atentan contra la seguridad de la información y la protección y privacidad de los datos, es fundamental que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un sistema de gestión de seguridad de la información basado en los riesgos y a su vez, alineado con los objetivos estratégicos y necesidades tanto de la organización como de sus partes interesadas.

CORVIVIENDA es consciente que la protección y seguridad de su información es fundamental para garantizar su debida gestión financiera, administrativa y operativa, razón por la cual debe establecer un marco normativo de Seguridad de la Información que contemple políticas, límites, responsabilidades y obligaciones frente a la seguridad y privacidad de la información de la entidad.

El presente documento contiene el plan de seguridad y privacidad de la información para el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de CORVIVIENDA, el cual tomará como referencia el Modelo de Seguridad y Privacidad de la estrategia de Gobierno en Línea y la norma ISO 27001, los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de un modelo de Gestión de Seguridad y Privacidad de la Información en cualquier tipo de organización, lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo.

# 2. OBJETIVOS

## 2.1. OBJETIVO GENERAL

Establecer un Plan de Seguridad y Privacidad de la Información que apoye el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de CORVIVIENDA, acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno en línea, los requerimientos de la entidad y en cumplimiento de las disposiciones legales vigentes.

## 2.2. OBJETIVOS ESPECÍFICOS

- Definir las etapas para establecer la estrategia de seguridad de la información de la entidad.
- Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno en Línea.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.

# 3. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD

## 3.1. CICLO DE OPERACIÓN

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea contempla el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

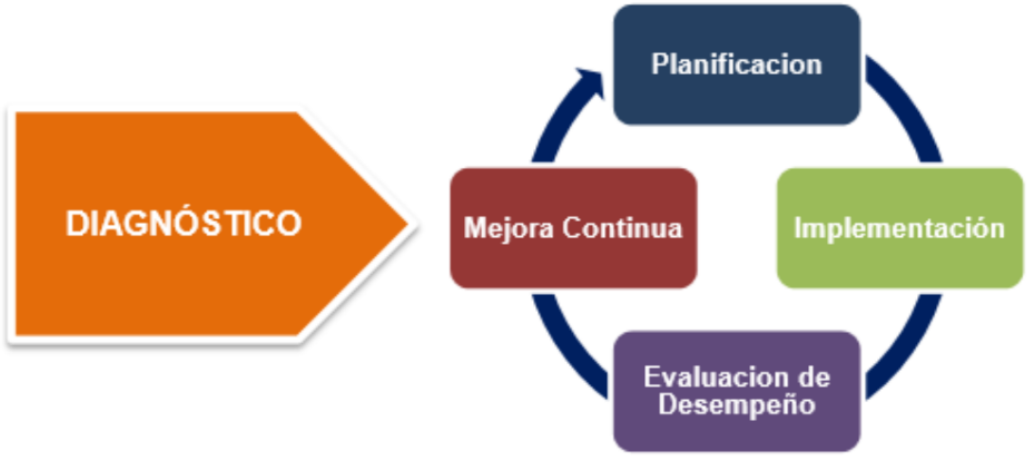


Figura 1. Ciclo de operación Modelo de Seguridad y Privacidad de la Información
Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

- **Fase Diagnostico**: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información .
- **Fase Planificación (P**lanear**):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- **Fase Implementación (H**acer**):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

- **Fase Evaluación de desempeño (V**erificar**):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

- **Fase Mejora Continua (A**ctuar**):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

### 3.2. ALINEACIÓN NORMA ISO 27001:2013 VS CICLO DE OPERACIÓN

Aunque en la norma ISO 27001:2013 no se determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:

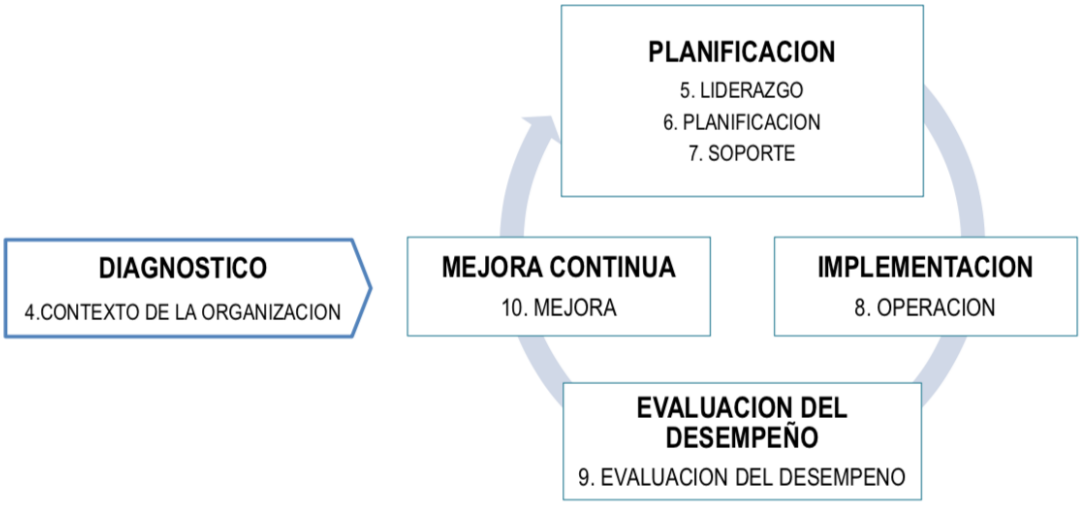


Figura 2. Norma ISO 27001:2003 alineado al Ciclo de mejora continua

Fuente: Elaborada con base en la información publicada en la página web http://www.welivesecuriry.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

El siguiente cuadro muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnostico, Planificación, Implementación, Evaluación, Mejora Continua) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

1.1.1.1.1 Tabla 1. Fases ciclo operación Vs estructura ISO 27001:2013

| **FASE** | **CAPITULO ISO 27001:2013** |
|---|---|
| Diagnóstico | Contexto de la Organización |
| Planificación | Liderazgos<br>Planificación<br>Soporte |
| Implementación | Operación |
| Evaluación de Desempeño | Evaluación de Desempeño |
| Mejora continua | Mejora |

- **Fase DIAGNOSTICO en la norma ISO 27001:2013.** En el **capítulo 4 - Contexto de la organización** de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del SGSI.
- **Fase PLANEACIÓN en la norma ISO 27001:2013**En el **capítulo 5 - Liderazgo***,* se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización asegure la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.En el **capítulo 6 - Planeación**, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.En el **capítulo 7 - Soporte** se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua Sistema de Gestión de Seguridad de la Información.
- **Fase IMPLEMENTACIÓN en la norma ISO 27001:2013.** En el **capítulo 8 - Operación** de la norma ISO 27001:2013*,* se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

- **Fase EVALUACIÓN DEL DESEMPEÑO en la norma ISO 27001:2013.** En el **capítulo 9 - Evaluación del desempeño,** se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

- **Fase MEJORA CONTINUA en la norma ISO 27001:2013.** En el **capítulo 10 - Mejora*,*** se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

### 3.3. FASE I: DIAGNÓSTICO

**Objetivo:** Identificar el estado de la Entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información

| **Metas** | **Actividades/Instrumentos/Resultados** |
|---|---|
| Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. | **Diagnóstico** de la **situación actual** de la entidad con relación a la gestión de seguridad de la información.**Diagnostico nivel de cumplimiento** de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la **norma ISO 27001:2013**.**Valoración estado actual** de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC. |
| Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad. | **Valoración** del **nivel de estratificación** de la entidad frente a la seguridad de la información **con base en** el método planteado en el documento '*ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES*' del modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0.<br>**Valoración** del **nivel de madurez** de seguridad y privacidad de la información en la entidad de acuerdo con los lineamientos establecidos en el capítulo '*MODELO DE MADUREZ*' del documento Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea. |
| Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación. | **Ejecución prueba de vulnerabilidades** con el fin de identificar el nivel de seguridad y protección de los activos de información de la entidad y definición de planes de mitigación. |

Para la recolección de la información, en esta fase se utilizarán mecanismo como:

- Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento de le entidad con relación a los dominios de la norma ISO/IEC 27001:2013.

- Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.

- Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

## 3.4. FASE II: PLANIFICACIÓN

**Objetivo:** Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del SGSI.

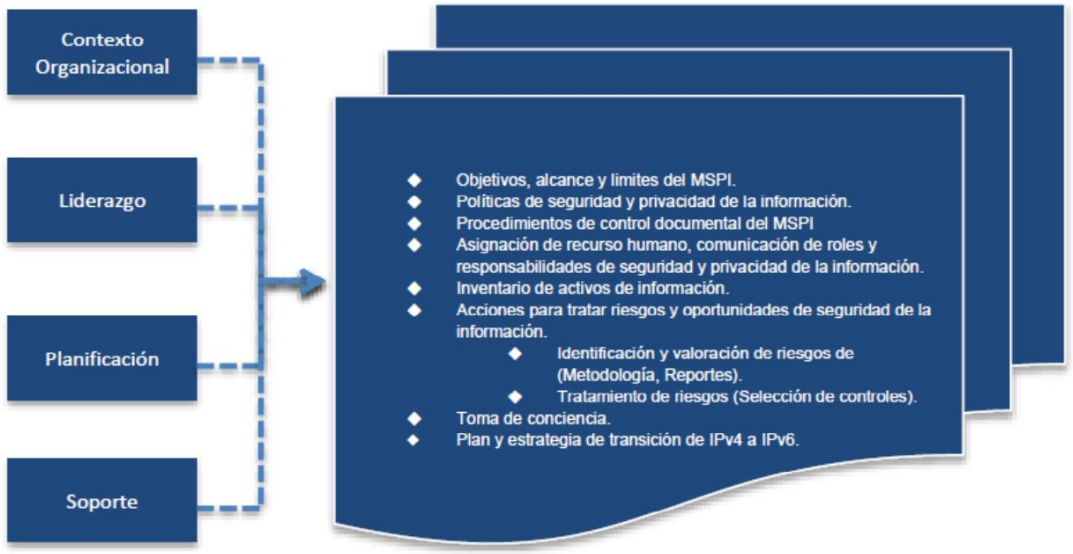


Figura 3. Fase de planificación modelo de seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

| **Metas** | **Actividades/Instrumentos/Resultados** |
|---|---|
| Realizar un análisis de Contexto y factores externos e internos de la Entidad en torno a la seguridad de la información. | Realizar un Análisis de Contexto de la entidad entorno a la seguridad de la información teniendo en cuenta el capítulo 4. CONTEXTO DE LA ORGANIZACIÓN de la norma ISO 27001:2013, con el fin de poder determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Sistema de Gestión de Seguridad de la Información. |
| Definir el alcance del SGSI de la entidad | Definir el alcance del Sistema de Gestión de Seguridad de la Información 'SGSI' de la entidad aprobado por la Alta Dirección y socializado al interior de la Entidad.Definir el alcance del SGSI, en el cual se establece los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información. |
| Definir roles, responsables y funciones de seguridad y privacidad de la información | Adicionar las funciones de seguridad de la información al Comité de Riesgos de la entidad y formalizarlas mediante acto administrativo.Establecer el Rol de Oficial de Seguridad de la información. Definir un marco de gestión que contemple roles y responsabilidades para la implementación, administración, operación y gestión |

| | |
|---|---|
| | de la seguridad de la información en la entidad. Definir la estructura organizacional de la Entidad que contendrá los roles y responsabilidad pertinentes a la seguridad de la información. |
| Definir la metodología de riesgos de seguridad de la información | Definir Metodología de Valoración de Riesgos de Seguridad. Integrar la metodología definida con la metodología de riegos operativos de la entidad.Implementar un sistema de información para la administración y gestión de los riesgos de seguridad de la entidad. |
| Elaborar las políticas de seguridad y privacidad de la información de la entidad | Elaborar Política General de Seguridad y Privacidad la cual debe ser aprobada por la Alta Dirección y socializada al interior de la Entidad.Elaborar el manual de Políticas de Seguridad y Privacidad de la Información, que corresponde a un documento que contiene las políticas y los lineamientos que se implementaran en la Entidad con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información. Estas políticas deben ser aprobadas por la Alta Dirección y socializadas al interior de la Entidad. |
| Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información | Elaborar los documentos de operación del sistema de seguridad de la información, tales como:<br>• Declaración de aplicabilidad<br>• Procedimiento y/o guía de identificación y clasificación de activos de información.<br>• Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI<br>• Procedimiento para control de documentos (SGI)<br>• Procedimiento para auditoría interna (SGI)<br>• Procedimiento para medidas correctivas (SGI)<br>• Procedimiento para la gestión de eventos e incidentes de seguridad de la información<br>• Procedimiento para la gestión de vulnerabilidades de seguridad de la información.<br>• Entre otros. |
| Identificar y valorar activos de información | Realizar la identificación y valoración de los activos de información de la entidad de acuerdo con su nivel de criticidad de acuerdo con el alcance del SGSI.Documentar el inventario de activos de información de la entidad. |
| Identificar, valorar y tratar los riesgos de seguridad de la información de la entidad | Realizar la identificación y valoración de los riesgos transversales de seguridad de la información y definir los respectivos planes de tratamiento.Realizar la |

| | |
|---|---|
| | valoración de riesgos de seguridad de la información de acuerdo con el alcance del SGSI.<br>Definir los planes de acción que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos. Para la seleccionar de los controles, se tomará como base los objetivos de control y los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013. |
| Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información. | Elaborar plan anual de capacitación y sensibilización anual de seguridad de la información |
| Establecer Plan de diagnóstico de IPv4 a IPv6 | Realizar el diagnóstico para la transición de la entidad de IPv4 a IPv6.Documentar el Plan de diagnóstico para la transición de IPv4 a IPv6. |

### 3.5. FASE III: IMPLEMENTACIÓN

**Objetivo:** Llevar acabo la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la entidad.


Figura 4. Fase de implementación modelo de seguridad

Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

| **Metas** | **Actividades/Instrumentos/Resultados** |
|---|---|
| Establecer el plan de implementación de seguridad de la información | Implementar el plan de implementación del modelo de seguridad y privacidad de la información el cual debe ser revisado y aprobado por el comité de riesgos |
| Ejecutar el plan de tratamiento de riesgos | Ejecutar el plan de tratamiento de los riesgos transversales de seguridad de la información identificados en la fase de planificación que fue presentado en el comité de riegos. |
| Ejecutar del plan y estrategia de transición de IPv4 a IPv6. | Ejecutar plan de transición a IPv6 y elaborar informe de implementación. |

| | |
|---|---|
| Establecer indicadores de gestión de seguridad | Definir los indicadores para medir la gestión del modelo de seguridad y establecer los mecanismos para su medición. Estos indicadores deben permitir verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos de seguridad de la entidad. |
| Implementar procedimiento de gestión de eventos e incidentes de seguridad | Implementar el procedimiento y los mecanismos para la gestión de los eventos e incidentes de seguridad de la información. |
| Implementar procedimiento de gestión de vulnerabilidades | Implementar el procedimiento y los mecanismos para la gestión de vulnerabilidades seguridad de la información. |
| Ejecutar plan de capacitación y sensibilización de seguridad | Ejecutar el plan anual de capacitación, socialización y sensibilización de seguridad de la información |
| Ejecutar pruebas anuales de vulnerabilidades e intrusión | Ejecutar el plan anual de pruebas vulnerabilidades e intrusión con el objetivo de identificar el nivel de protección de los activos de información de la entidad. Para tal efecto, se deberá tener en cuenta los respectivos requerimientos de seguridad relacionados con pruebas de vulnerabilidades establecidos en la circular externa 029 de 2014 de la Superfinanciera de Colombia o la circular que las reemplacen. |
| Ejecutar pruebas de Ethical Hacking | Ejecutar pruebas anuales de Ethical Hacking orientadas a poder determinar los niveles de riesgo y exposición de la organización ante atacantes interno o externo que puedan a comprometer activos críticos de la entidad y con esto generar interrupción en los servicios, afectar la continuidad del negocio y/o acceder de forma no autorizada a la información sensible o clasificada de la entidad o de carácter personal de los trabajadores o terceros que laboren para la entidad. |
| Ejecutar pruebas de Ingeniera Social | Ejecutar pruebas anuales de ingeniería social orientadas a verificar aspectos como: (i) los protocoles internos de seguridad, (ii) el nivel de concientización de los funcionarios y terceros que laboren en la entidad sobre temas de seguridad de la información, (iii) el conocimiento y/o cumplimiento de las políticas de seguridad y privacidad de la información de la entidad y (iv) el nivel de exposición de la información publicada en internet de la entidad y de sus empleados. |

### 3.6. FASE IV: EVALUACIÓN DE DESEMPEÑO

**Objetivo:** Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permita determinar la efectividad de la implantación del SGSI.

Figura 5. Fase Evaluación Desempeño modelo de seguridad

Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

| Metas | Actividades/Instrumentos/Resultados |
|---|---|
| Ejecución de auditorías de seguridad de la información | Ejecución de auditorías del modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, de acuerdo con el plan de auditoria revisado y aprobado por la Alta Dirección.<br>Las auditorías internas se deberán llevar a cabo para la revisión del Sistema de Gestión de Seguridad 'SGSI' de la Información implementado en la entidad, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del SGSI cumpla con los requisitos establecidos en la norma ISO 27002:2013 y los del MSPI. |
| Plan de seguimiento, evaluación y análisis de SGSI | Elaboración documento con el plan de seguimiento, evaluación y análisis del SGSI revisado y aprobado por el Comité de Riesgos. |

### 3.7. FASE V: MEJORA CONTINUA

**Objetivo:** Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI


Figura 6. Fase Mejora Continua modelo de seguridad

Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

| Metas | Actividades/Instrumentos/Resultados |
|---|---|
| Diseñar plan de mejoramiento | Diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el Sistema de Gestión de Seguridad de la Información. |

## 4. TÉRMINOS Y REFERENCIAS

**Activo de información**: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

**Amenaza**: Es la causa potencial de un daño a un activo de información.

**Anexo SL**: Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

**Análisis de riesgos**: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

**Causa**: Razón por la cual el riesgo sucede.**Ciclo de Deming**: Modelo mejora continua para la implementación de un sistema de mejora continua.

**Colaborador:** Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.

**Confidencialidad**: Propiedad que determina que la información no esté disponible a personas no autorizados

**Controles**: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

**Disponibilidad**: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

**Dueño del riesgo sobre el activo**: Persona responsable de gestionar el riesgo.**Impacto**: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

**Incidente de seguridad de la información:** Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

**Integridad**: Propiedad de salvaguardar la exactitud y estado completo de los activos.

**Oficial de Seguridad**: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

**Probabilidad de ocurrencia**: Posibilidad de que se presente una situación o evento específico.

**Responsables del Activo**: Personas responsables del activo de información.

**Riesgo**: Grado de exposición de un activo que permite la materialización de una amenaza.

**Colaborador:** Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.

**Riesgo Inherente**: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

**Riesgo Residual**: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.
**PSE:** Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.

**SARC**: Siglas del Sistema de Administración de Riesgo Crediticio. **SARL**: Siglas del Sistema de Administración de Riesgo de Liquidez.

**SARLAFT**: Siglas del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo.

**SARO**: Siglas del Sistema de Administración de Riesgos Operativos.**Seguridad de la Información**: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

**SGSI**: Siglas del Sistema de Gestión de Seguridad de la Información.

**Sistema de Gestión de Seguridad de la información SGSI:** permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

**Vulnerabilidad**: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotad