



**MODELO DE SEGURIDAD DE LA  
INFORMACIÓN Y CIBERSEGURIDAD -  
MSIC**

**VERSIÓN: 1**

**PÁGINA 1 DE 18**

# **MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD**

**IDEA**



# MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC

VERSIÓN: 1

PÁGINA 2 DE 18

<b>INTRODUCCIÓN.....</b>	<b>4</b>
<b>1. OBJETIVO.....</b>	<b>4</b>
<b>2. ALCANCE.....</b>	<b>4</b>
<b>3. DEFINICIONES .....</b>	<b>5</b>
<b>4. CICLO DE OPERACIÓN.....</b>	<b>7</b>
<b>5. Fase de Diagnostico .....</b>	<b>8</b>
<b>5.1 Instrumento de Evaluación del MSIC .....</b>	<b>8</b>
5.1.1 Levantamiento de información .....	8
5.1.2 Pruebas y análisis.....	8
5.1.3 Informes y recomendaciones .....	9
<b>5.2 Autodiagnóstico Gobierno Digital - MIPG .....</b>	<b>10</b>
<b>6. Fase de Planificación.....</b>	<b>11</b>
<b>6.1 Política de Seguridad de la Información y Ciberseguridad .....</b>	<b>11</b>
- Directrices para la Seguridad de la Información y la Ciberseguridad .....	11
- Roles y Responsabilidades de Seguridad de la Información y Ciberseguridad.....	11
<b>6.2 Procedimientos de Seguridad de la Información y Ciberseguridad.....</b>	<b>11</b>
6.2.1 Seguridad de los Recursos Humanos.....	12
6.2.2 Gestión de Activos .....	12
6.2.3 Riesgos de Seguridad de la información y Ciberseguridad .....	12
6.2.4 Control de Acceso .....	13
6.2.5 Procedimiento de Gestión de Incidentes de Seguridad de la Información .....	13
6.2.6 Seguridad Física y del Entorno.....	14
6.2.7 Guía de Endurecimiento (Hardening) .....	14
6.2.8 Seguridad de las Operaciones .....	15
6.2.9 Seguridad de las Comunicaciones .....	15
6.2.10 Gestión de la Continuidad de la Seguridad del Negocio .....	15



# MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC

VERSIÓN: 1

PÁGINA 3 DE 18

<b>7.</b>	<b><i>Fase de Implementación .....</i></b>	<b><i>17</i></b>
<b>8.</b>	<b><i>Fase de Evaluación de Desempeño .....</i></b>	<b><i>17</i></b>
8.1	Guía Evaluación de Desempeño .....	17
8.2	Guía de Auditoría .....	18
<b>9.</b>	<b><i>Fase de Mejora Continua .....</i></b>	<b><i>18</i></b>
9.1	Guía de Mejora Continua .....	18



## **MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC**

**VERSIÓN: 1**

**PÁGINA 4 DE 18**

### **INTRODUCCIÓN**

El Modelo de Seguridad de la Información Y Ciberseguridad, encamina al Instituto a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo mantener la privacidad de los datos.

El Modelo operará a través de las siguientes 5 fases; diagnostico, planificación, implementación, evaluación de desempeño y mejora continua.

Las fases incluirán objetivos, metas, procedimientos y seguimientos, permitiendo que la seguridad de la información y la ciberseguridad sean un sistema de gestión sostenible.

El Modelo será revisado con regularidad, dado que forma parte del Modelo Integrado de Planeación y Gestión -MIPG-; por lo tanto, al identificar cambios en la normatividad en el negocio, en su estructura, objetivos o en general, deberá actualizarse y así asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

### **1. OBJETIVO**

Estructurar un Modelo de Seguridad de la Información y Ciberseguridad, aplicando lineamientos de buenas prácticas que permitan proteger y minimizar los riesgos en los activos de información, para brindar credibilidad y confianza en nuestros clientes.

### **2. ALCANCE**

El Modelo de Seguridad de la Información Y Ciberseguridad es aplicable a todos los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la información del Instituto para el desarrollo de Antioquia – IDEA-, por consiguiente, aplicará a la estructura del Modelo de Operaciones por Procesos del Instituto.

Para el logro del objetivo, los usuarios tienen la obligación de dar cumplimiento a todos los lineamientos descritos en el Modelo, aportando con su participación en la toma de medidas preventivas y correctivas.



## MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC

VERSIÓN: 1

PÁGINA 5 DE 18

### 3. DEFINICIONES

**Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

**Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

**Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

**Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

**Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

**Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

**Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

**Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

**Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)



## **MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC**

**VERSIÓN: 1**

**PÁGINA 6 DE 18**

**Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

**Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.

**Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

**Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

**Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

**Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

**Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

**Sistema de Gestión de Seguridad de la Información:** SGSI Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación

de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

**Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

**Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

**Partes interesadas (Stakeholder)** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

#### **4. CICLO DE OPERACIÓN**

El funcionamiento del Modelo de Seguridad de la Información Y Ciberseguridad se desarrollará en las siguientes 5 fases:

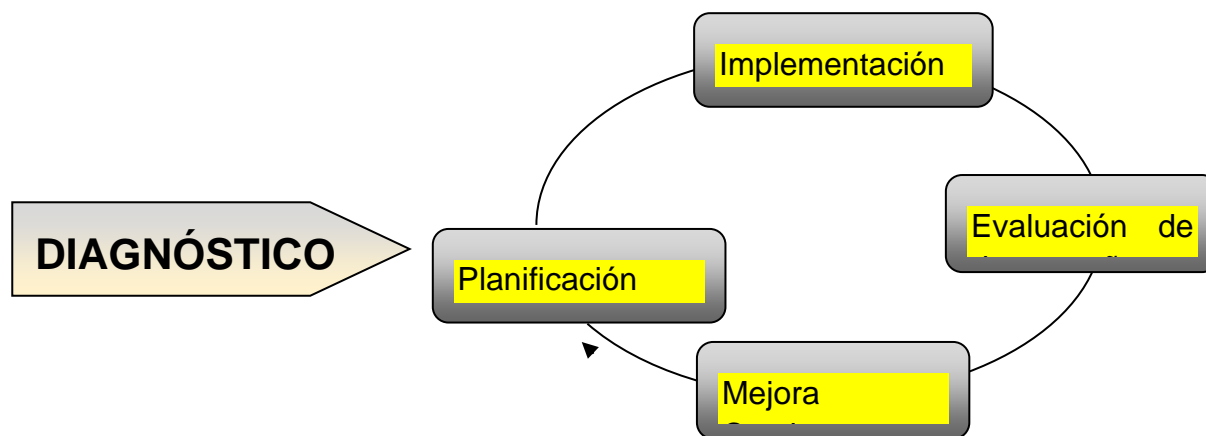



Figura 1. Ciclo de Operación

	<b>MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC</b>	<b>VERSIÓN: 1</b>
		<b>PÁGINA 8 DE 18</b>

## 5. Fase de Diagnostico

En esta fase se pretende diagnosticar el estado del grado de madurez de los controles institucionales. Se identificará cual es el estado actual del IDEA frente a las seguridad y privacidad de la información.

### 5.1 Instrumento de Evaluación del MSIC

Este Instrumento, es la herramienta de diagnóstico para conocer el estado actual de la gestión de la seguridad y privacidad de la información en el Instituto, así como, el nivel de madurez de los controles de seguridad utilizados.

La ejecución de la evaluación se realizó en las siguientes fases:

#### 5.1.1 Levantamiento de información

se recopila todos los datos e información necesaria para realizar la evaluación:

- Áreas Involucradas: Se involucran en el proceso de autoevaluación el área o responsable, el tema a tratar y el funcionario que debe apoyar el desarrollo del tema.

#### 5.1.2 Pruebas y análisis


- Pruebas Administrativas: Se recopila temas de seguridad de la información de las áreas que no están directamente relacionadas con las áreas tecnológicas del Instituto, así como Políticas de Seguridad, Responsabilidades y acuerdos de confidencialidad.
- Pruebas Técnicas: se evalúan algunos controles de la Norma ISO 27001, requisitos del Modelo de Seguridad y Privacidad de la Información de Mintic, Gobierno Digital y mejores prácticas de ciberseguridad.
- Avance PHVA: se determina el nivel de cumplimiento del ciclo PHVA del Modelo, incluyendo los siguientes componentes:

Planificación

Implementación

Evaluación de desempeño



	<b>MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC</b>	<b>VERSIÓN: 1</b>
		<b>PÁGINA 9 DE 18</b>

#### Mejora Continua

- Ciberseguridad: se determina como se encuentra el Instituto frente a las mejores prácticas en ciberseguridad.

#### 5.1.3 Informes y recomendaciones

- Madurez: se identifican cada uno de los requisitos que se requieren para cumplir los niveles de madurez del MSIC. Estos requisitos ya fueron previamente evaluados en la fase de administrativa, técnicas y PHVA. También hay otros requisitos (3) que se evaluaron manualmente.
- Brecha Anexo ISO 27001:2013

En este componente se muestra el resultado del análisis de brecha frente a los controles del Anexo A, del estándar ISO 27001:2013, y la guía de controles (Guía #8) del Modelo de Seguridad de Privacidad de la Información el cuadro de resumen y la gráfica se construyen automáticamente en la medida que se diligencia el Instrumento.

- Escala de Evaluación

Muestra la posible calificación que se puede dar a cada criterio:



## MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC

VERSIÓN: 1

PÁGINA 10 DE 18

Tabla de Escala de Valoración de Controles		
Descripción	Calificación	Criterio
Aplica	N/A	No aplica.
Existente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Detenable	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Activo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Monitoreado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Automatizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

### - Avance del MSIC del IDEA

Se muestra la calificación obtenida en cada requisito solicitado y proviene en casi todos los casos de las calificaciones otorgadas por el evaluador en las hojas Administrativas, Técnicas y PHVA, y en solo 3 casos se califica de acuerdo a la Escala de Evaluación.

## 5.2 Autodiagnóstico Gobierno Digital - MIPG

La herramienta de diagnóstico que trae el Modelo Integrado de Planeación y Gestión- MIPG, estos son los resultados referentes a la seguridad y privacidad de la información

De acuerdo a los resultados, se inicia un plan de mejoramiento para mejorar la calificación.



## **MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC**

**VERSIÓN: 1**

**PÁGINA 11 DE 18**

### **6. Fase de Planificación**

Basados en los resultados obtenidos en la fase de diagnóstico, se procede a elaborar el Plan de Seguridad de la Información y Ciberseguridad, con el propósito de definir acciones a implementar, a través de una metodología de gestión del riesgo.

La fase de planificación estará conformada por las siguientes procedimientos, planes y guías, los cuales deberán estar alineados con el objetivo misional del Instituto:

#### **6.1 Política de Seguridad de la Información y Ciberseguridad**

Se debe establecer y documentar una Política de Seguridad de la Información y Ciberseguridad, la cual debe ser aprobada por la Junta Directiva del Instituto.

La Política debe ser aprobada y divulgada al interior del Instituto.

- Directrices para la Seguridad de la Información y la Ciberseguridad

Es el manual de Políticas, que garantizará el adecuado uso de activos de información al interior del Instituto; definiendo responsabilidades generales y específicas para la gestión de la seguridad de la información y la ciberseguridad.

- Roles y Responsabilidades de Seguridad de la Información y Ciberseguridad

El Instituto debe definir los roles y las responsabilidades para la Seguridad de la Información y Ciberseguridad en los diferentes niveles (directivo, de procesos y operativos) que permitan la correcta toma de decisiones y una adecuada gestión para el cumplimiento de los objetivos Institucionales.

#### **6.2 Procedimientos de Seguridad de la Información y Ciberseguridad**

En este procedimiento se desarrollarán y formalizarán procedimientos que permitan gestionar la Seguridad de la Información y Ciberseguridad en cada uno de los procesos.



## **MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC**

**VERSIÓN: 1**

**PÁGINA 12 DE 18**

### **6.2.1 Seguridad de los Recursos Humanos**

Propósito: Asegurarse que los funcionarios, contratistas y terceros comprendan sus responsabilidades de seguridad de la información, protegiendo siempre los intereses del Instituto después de la terminación del contrato.

- Plan de Sensibilización para la Seguridad de la Información y Ciberseguridad: El instituto debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información y la ciberseguridad se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) del Instituto.

### **6.2.2 Gestión de Activos**


Propósito: Identificar los activos de información del Instituto y definir responsabilidades para su protección y divulgación.

- Guía para la gestión de activos de información: El Instituto debe desarrollar una metodología para la gestión de activos de información, que permita tener un inventario de activos de información exacto y actualizado, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

### **6.2.3 Riesgos de Seguridad de la información y Ciberseguridad**

Propósito: Establecer un marco de administración de riesgos de seguridad de la información y ciberseguridad, que permita identificar las amenazas y vulnerabilidad que puedan afectar la confidencialidad, integridad y disponibilidad de la información del Instituto.

- Sistema de Administración de Riesgo de Seguridad de la Información y Ciberseguridad: El Instituto deberá definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad.

	<b>MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC</b>	<b>VERSIÓN: 1</b>
		<b>PÁGINA 13 DE 18</b>

#### 6.2.4 Control de Acceso

Propósito: Definir directrices que permitan que los mecanismos de protección utilizados por el Instituto limiten el acceso a la información y eviten accesos no autorizados a sistemas y aplicaciones.

- Guía Prevención de Fuga de Información: Se definirán políticas para el acceso a la información, toda el Instituto deberá seguir el principio de mínimo privilegio, en que un usuario sólo debe tener acceso a la información estrictamente necesaria para desempeñar sus funciones diarias, siempre que no referimos a información confidencial.
- Guía de Disposición Final de la Información: Esta guía definirá la gestión que se le realizará a los recursos que ya no van a ser utilizados (traslado, donación, entre otros) teniendo en cuenta que la información tiene una vida útil, tanto si está en formato digital (CD, DVD, Usb, Discos, tarjetas de memoria, entre otros) o en formatos tradicionales (papel, películas, dispositivos de backup, entre otros.).
- Procedimiento Administración de Identidades y Accesos: En este procedimiento, el Instituto indicará como se realizará la creación de usuarios y la asignación de contraseñas. Se debe aplicar a todos los sistemas de información, también se debe tener en cuenta el rol que cada usuario requiera en los determinados sistemas, para brindar el acceso necesario.

#### 6.2.5 Procedimiento de Gestión de Incidentes de Seguridad de la Información

Propósito: Gestionar los incidentes de seguridad de la información y comunicar los eventos de seguridad.

Este procedimiento debe indicar como responde el Instituto en caso de presentarse algún incidente que afecte alguno de los 3 servicios fundamentales de la información: Disponibilidad, Integridad o confidencialidad.

Deben especificarse los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información, así mismo, deberá indicar en qué casos sería necesario pasar a la activación de los planes de BCP (Planes de Continuidad del negocio) dependiendo de la criticidad de la información.

Esta guía deberá contener lecciones aprendidas.



## **MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC**

**VERSIÓN: 1**

**PÁGINA 14 DE 18**

### **6.2.6 Seguridad Física y del Entorno**

Propósito: Prevenir el acceso físico no autorizado a las instalaciones de procesamiento de información y el daño, pérdida o robo de los activos de información.


- Procedimiento de Seguridad Física y del entorno: En este procedimiento se debe describir cómo se ejecutan los diferentes pasos para garantizar el control de acceso seguro a las instalaciones al personal autorizado. Este procedimiento puede incluir registros de fecha y hora de ingreso, seguimiento de los libros o plataforma de registro. Se debe contemplar la solicitud de permiso a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a las áreas, entre otros. En este procedimiento también incluye:

Protección de Activos: Son los pasos con los cuales los equipos son protegidos en el Instituto. Se debe indicar como se determina la ubicación de los equipos que procesan información confidencial, como se aseguran dichas instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños, por polvo, agua, interferencias, descargas eléctricas, entre otros.

Retiro de Activos: Se especifica como los activos son retirados del Instituto con previa autorización. Se debe indicar el control que tendrá el activo fuera en el Instituto, así como también los controles de seguridad que deberá incluir el equipo cuando esté por fuera (controles criptográficos, cifrado de discos, entre otros).

### **6.2.7 Guía de Endurecimiento (Hardening)**

se deberán realizar una serie de actividades, para disminuir al máximo la superficie de ataque de los sistemas y dispositivos, realizando instalaciones seguras de los sistemas operativos, eliminando lo que no necesitan las máquinas (Lockdown) y proporcionando lo que se necesita para que presten los servicios de manera segura (Lockup).

	<b>MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC</b>	<b>VERSIÓN: 1</b>
		<b>PÁGINA 15 DE 18</b>

#### 6.2.8 Seguridad de las Operaciones

Propósito: Se debe asegurar que los procedimientos de las operaciones que procesen información se realicen de forma correcta y segura, y permitan el registro de eventos.

- Procedimiento de Gestión de Cambios: Se debe documentar como se realiza la Gestión de Cambio en el Instituto, en los procesos de negocio y en los sistemas de información de manera segura. Se deben especificar aspectos como identificación y registro de cambios significativos, planificación y pruebas previas de los cambios a realizar, valoración de impactos, tiempos de no disponibilidad del servicio, comunicación a las áreas pertinentes, procedimientos de rollback (reversa), entre otros.

#### 6.2.9 Seguridad de las Comunicaciones

Propósito: Asegurar la protección de la información en las redes y mantener la seguridad de la información transferida dentro del Instituto y con cualquier entidad externa.

- Guía de Seguridad de Proyectos Críticos: Se presentarán lineamiento y aspectos a tener en cuenta para el aseguramiento de la información en la nube (cloud), reduciendo el riesgo de que se presenten incidentes de seguridad.

Este procedimiento debe indicar como el Instituto establece, acuerda, aprueba y divulga los requerimientos y obligaciones relacionados con la seguridad de la información, tanto con los proveedores como con la cadena de suministros que estos tengan (es decir algún intermediario). Dichos acuerdos deben tener características como: Aspectos legales, descripción de la información a la que ambas partes tendrán acceso, reglas de uso aceptable e inaceptable de la información, requerimientos en gestión de incidentes, resolución de conflictos, informes periódicos por parte del proveedor, auditorías al servicio y gestión de cambios.

#### 6.2.10 Gestión de la Continuidad de la Seguridad del Negocio

Propósito: La continuidad de la seguridad de la información debe estar incluida en el Plan de Continuidad de negocio del IDEA.



# **MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC**

**VERSIÓN: 1**

**PÁGINA 16 DE 18**

N°	INSTRUMENTO	RESPONSABLE	1° SEMESTRE 2023						2° SEMESTRE 2023					
			E	F	M	A	M	J	J	A	S	O	N	D
1	Modelo de Seguridad de la Información y Ciberseguridad (MSIC)	La Oficina Gestión del Riesgo, Dirección de Sistemas y Comité de Seguridad de la Información y Ciberseguridad.	X	X	X	X	X	X	X	X	X	X	X	X
2	Política de Seguridad de la Información y Ciberseguridad	La Oficina Gestión del Riesgo, Dirección de Sistemas y Comité de Seguridad de la Información y Ciberseguridad.		X	X	X	X	X						
3	Plan de Sensibilización para la Seguridad de la Información y Ciberseguridad	La Oficina Gestión del Riesgo, Oficina Asesora de Comunicaciones y Comité de Seguridad de la Información.		X	X				X	X	X			
4	Guía para la Gestión de Activos de Información	La Oficina Gestión del Riesgo y Centro de Administración Documental.			X			X			X			
5	Sistema de Administración de Riesgo de Seguridad de la Información y Ciberseguridad	La Oficina Gestión del Riesgo y Comité de Seguridad de la Información.		X	X	X	X	X	X	X	X	X		
6	Guía para la prevención de Fuga de Información	La Oficina Gestión del Riesgo, Oficina Asesora de Comunicaciones y Comité de Seguridad de la Información.		X	X	X	X	X						
7	Guía para la Disposición Final	Dirección de Sistemas y Centro de Administración Documental.										X		
8	Procedimiento gestión de identidades y accesos	La Oficina Gestión del Riesgo y Dirección de Sistemas				X	X							
16	Procedimiento de Gestión de Incidentes de Seguridad	Equipo de Respuesta de Incidentes	X	X	X	X	X	X	X	X	X	X	X	X
10	Procedimiento de Seguridad Física y del Entorno	La Oficina Gestión del Riesgo, Dirección de Sistemas y Subgerencia Administrativa.			X			X			X			
14	Guía de Hardening (Endurecimiento)	La Oficina Gestión del Riesgo y Dirección de Sistemas			X	X	X	X	X					



11	Procedimiento de Gestión de Cambios	Oficina de Planeación, Oficina Gestión del Riesgo, Dirección de Sistemas y Comité de Seguridad de la Información y Ciberseguridad.								X	X	X					
13	Guía de Seguridad Proyectos Críticos	La Oficina Gestión del Riesgo, Dirección de Sistemas y Dirección Técnica Contractual.			X			X									
17	Plan de Continuidad del Negocio (Seguridad)	Equipo de Respuesta de Incidentes	X	X	X	X	X	X									

## 8.1 Guía Evaluación de Desempeño



## **MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - MSIC**

**VERSIÓN: 1**

**PÁGINA 18 DE 18**

### **8.2 Guía de Auditoría**

El Instituto debe generar un documento donde se especifique el plan de auditorías para el MSIC, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Se debe llevar a cabo auditorías y revisiones independientes a intervalos planificados que permitan identificar si el MSIC es está implementado adecuadamente y se mantiene de forma eficaz; así mismo es necesario difundir a las partes interesadas, los resultados de la ejecución de las auditorías.

Es importante conservar la información documentada como evidencia de los resultados de las auditorías.

### **9. Fase de Mejora Continua**

En esta fase el Instituto deberá consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad de la información y ciberseguridad, tomando las acciones oportunas para mitigar las debilidades identificadas.

#### **9.1 Guía de Mejora Continua**

En esta fase es importante que el Instituto defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño.