PLAN DE TRATAMIENTO DE RIESGOS

2023

SEGURIDAD Y PRIVACIDAD DE LA INFIORMACIÓN

GOBERNACIÓN DE SANTANDER

INDER Santander

CONTENIDO

INTRODUICCIÓN

Durante el segundo semestre del año 2020, el Consejo Nacional de Política Económica y Social, publico el Documento CONPES 3995 sobre POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL, el cual resalta que “El entorno digital es un escenario en el que globalmente se desarrollan cada vez más todo tipo de actividades socioeconómicas. Esto expone tanto a las personas como a las mismas organizaciones a amenazas cibernéticas por parte de delincuentes que aprovechan el creciente intercambio de información. Se debe apuntar a que existan las medidas suficientes, tanto en el fortalecimiento de la seguridad, como en la generación de la confianza digital, respecto a una adecuada anticipación, gestión de riesgos, atención oportuna y defensa ante las amenazas existentes en el entorno digital, dentro de un marco de gobernanza nacional eficiente, acorde con las necesidades actuales y en constante desarrollo, en el que se pueda materializar rápidamente la confianza y la seguridad digital ante la aparición de nuevas tecnologías .”

Ilustración 1. Implementación de Políticas y estrategias desde el Gobierno Nacional para brindar seguridad y defensa en el ciberespacio. Fuente: Elaboración DNP, 2020

Bajo este marco de trabajo INDERSANTANDER presenta su plan de tratamiento de riesgos de seguridad digital para la vigencia 2023.

1.OBJETIVOS

1.1. OBJETIVO GENERAL

Determinar las acciones de tratamiento de riesgos de seguridad y privacidad de la información, mediante la identificación, análisis, valoración y tratamiento de los riesgos de pérdida de confidencialidad, disponibilidad e integridad de la información, para prevenir su materialización y/o reducir los impactos negativos en la gestión institucional.

1.2. OBJETIVOS ESPECÍFICOS

• Mejorar continuamente los conocimientos del equipo de trabajo en materia de seguridad digital y prevención de riesgos.
• Preparar a todos los colaboradores para responder ante incidentes de seguridad que afecten los activos de información.
• Mejorar la confianza de los grupos de valor en nuestra capacidad institucional para preservar la seguridad de la información.

2.RESPONSABILIDADES

Indersantander apoyará la implementación del plan de tratamientos de riesgos de Seguridad y Privacidad de Información como un proceso transversal incluido en el Comité Institucional de Gestión y Desempeño

Por lo anterior, se deben tener en cuenta al responsable de Tecnologías de la Información y Seguridad Digital de la Administración en las reuniones del Comité Institucional de Gestión y Desempeño.

3. TRATAMIENTO DE RIESGOS

3.1. Factores de riesgo

Para la vigencia 2023 se priorizan los siguientes factores de riesgo digital en nuestro plan de tratamiento de riesgos:

• Nivel de conocimiento del personal en amenazas digitales, políticas y controles de seguridad

• Disponibilidad permanente de servicios esenciales como telecomunicaciones, energía e infraestructura

• Identificación y protección de los datos de carácter personal

• Adecuada clasificación de la información bajo custodia de la Entidad de acuerdo con el marco legal vigente

• Entorno global digital inseguro

• Aislamiento forzoso del personal en sus residencias

• Segregación apropiada de roles y privilegios en todos los sistemas de información.

	TIPOLOGIA DE ACTIVOS
TIPO DE ACTIVO	***DESCRIPCIÓN***
Informacion	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Activos informáticos lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros
Componentes de red	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Personas	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades

3.2. Identificación del riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

3.2. Valoración del riesgo

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y valorándolos con el fin de obtener información para establecer su nivel y las posibles acciones a implementar.

Dicho análisis incluye las fuentes, así como los factores que generan las consecuencias y aumentan la probabilidad de que ocurran. En la etapa de análisis se identifican los controles existentes ya sean administrativos, técnicos y/o procedimientos implementados en la entidad. Por lo tanto, se analiza el riesgo combinando estimaciones de impacto y probabilidades en el contexto de las medidas de control existente.

La aplicación de análisis cualitativo facilita la calificación y evaluación de los riesgos al aplicar formas descriptivas para presentar la magnitud de las consecuencias potenciales (consecuencia) y la posibilidad de ocurrencia (probabilidad).

La valoración de los riesgos se realizará conforme a la Guía para la administración del riesgo y el diseño de controles en entidades públicas, reglamentada por el DAFP, en versión 05 de 2020.

3.3. Estrategia de tratamiento de riesgo

Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se puede evidenciar cuatro opciones:

Transferir: Son procedimientos que permiten eliminar el riesgo por medio de la transferencia.

Mitigar: Permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo puede reducirse a través de

controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.

Evitar: Puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado.

Aceptar: consiste en hacer frente a un riesgo (positivo o negativo) o porque no se ha identificado ninguna otra estrategia de respuesta adecuada.

La estrategia de control de riesgos para la vigencia 2023, contempla cuatro ejes que son: conocimiento, continuidad, control de acceso y controles tecnológicos, así:

3.3.1 Estrategias Orientadas al Conocimiento (Capacitación)

Mediante actividades de inducción, sensibilización y capacitación periódica se busca que todos los servidores y contratistas apropien conocimientos en materia de:

- Ley de protección de datos personales
- Ley de transparencia y acceso a la información
- Políticas institucionales de seguridad digital
- Modalidades y control de ataques informáticos
- Uso seguro de los recursos informáticos

3.3.2 Estrategias Orientadas al Conocimiento (Riesgos)

Para afrontar escenarios de riesgo asociados a la pérdida de continuidad, la Entidad adelantará en la vigencia 2023, acciones específicas en materia de:

- Fortalecimiento de su infraestructura de servicios básicos de energía

- Mejoramiento de sus capacidades de detección oportuna de eventos adversos de seguridad de la información.

3.3.3 Estrategias orientadas al conocimiento (Controles)

Con el fin de prevenir y controlar el acceso no autorizado a activos de información clasificados y reservados la Entidad emprenderá en la vigencia 2023 acciones específicas para:

- Actualizar los instrumentos de acceso a la información pública
- Reforzar los controles de acceso a activos de información con roles y privilegios más precisos.
- Reforzar el cumplimiento de los acuerdos de confidencialidad y los acuerdos de intercambio seguro de información

3.3.4 Estrategias de fortalecimiento de controles técnicos

Ante el aumento del tipo y complejidad de amenazas informáticas la entidad implementará estrategias específicas en:

- Identificación de eventos potencialmente nocivos
- Reforzamiento de controles de acceso a servicios en la nube
- Verificación y control de copias de respaldo
- Control de cambios en plataformas tecnológicas

8.Plan de Acción 2023

EJE	DESCRIPCIÓN	RESPONSABLE	ENTREGABLE	1 SEMESTRE						2 SEMESTRE					
				E	F	M	A	M	J	J	A	S	O	N	D

Riesgos	Actualización de los lineamientos de Riesgos de Seguridad de la Información en la Política de administración del Riesgos institucional.	CPS TIC CPS MIPG	Política Actualizada												
	Incluir dentro del plan de capacitación-PIC 2023 los riesgos de Seguridad digital y privacidad de la información.	CPS MIPG AÉREA DE TALENTO HUMANO	Registro del PIC 2023												
	Establecer reuniones con los líderes de los procesos previamente identificando los Riesgos de Seguridad de la Información por proceso.	CPS TIC CPS MIPG	Riesgos de seguridad digital por proceso												
	Socializar los Riesgos de	CPS TIC CPS MIPG	Registro de asistencia del comité												

	Seguridad de la Información ante el Comité Institucional de Gestión y Desempeño														
	Realizar monitoreo al cumplimiento de las acciones de control los Riesgos de Seguridad de la Información de la Entidad.	CPS TIC CPS MIPG	Informe de monitoreo												
	Realizar informe de Seguimiento al cumplimiento de las acciones de control los Riesgos de Seguridad de la Información de la Entidad.	Jefe de Control interno	Informe semestral de seguimiento												

BIBLIOGRAFÍA

- Decreto 103 de 2015 el cual reglamenta la ley 1712 de 2014 Ley de Transparencia.

- Ley 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y por el Decreto 1081 de 2015, Protección de datos personales

- Decreto único reglamentario 1078 de 2015 – MinTic – Modelo de Seguridad y Privacidad de Información.

- ISO/IEC 27000:2013. Estándar del Sistema de Gestión de Seguridad de Información.

Aprobó: Comité Institucional de Gestión y Desempeño.