



## PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**Proceso:** Gestión de TICS

2024

### CONTENIDO

**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14  
PBX: (60 1) 639 7888  
**IPSE Centro Nacional de Monitoreo:** (60 1) 6101130  
ipse@ipse.gov.co  
Bogotá D.C. – Colombia

Página | 1

1. GENERALIDADES DEL PLAN INSTITUCIONAL .....	3
1.1. Introducción .....	3
1.2. Alcance.....	3
1.3. Objetivos .....	4
1.3.1. Objetivo general .....	4
1.3.2. Objetivos específicos.....	4
2. CONTEXTO ESTRATÉGICO .....	4
3. MARCO CONCEPTUAL .....	5
4. MARCO NORMATIVO.....	8
5. DESCRIPCIÓN DEL PLAN.....	9
5.1. Establecimiento del contexto .....	9
5.2. Identificación del riesgo .....	9
5.3. Valoración del riesgo .....	10
5.4. Definición y aprobación de mapas de riesgos y planes de tratamiento. ....	11
5.5. Materialización.....	11
5.6. Oportunidad de Mejora .....	11
6. CRONOGRAMA DE SEGUIMIENTO Y EVALUACIÓN.....	11

## **1. GENERALIDADES DEL PLAN INSTITUCIONAL**

### **1.1. Introducción**

El Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información de Corvivienda está orientado a realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Adicionalmente dar los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en el Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas – IPSE.

El Plan de Tratamiento de Riesgo tendrá en cuenta todos los riesgos en especial los que se encuentren en los niveles Moderado, Alto y Extremo acorde con los lineamientos definidos por el Ministerio de TIC, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

### **1.2. Alcance**

Mediante la definición del Plan de Tratamiento de Riesgos se busca establecer medidas para mitigar los riesgos presentes en su análisis (pérdida de confidencialidad, pérdida de integridad y pérdida de disponibilidad de los activos de información) evitando situaciones que generen incertidumbre en el cumplimiento de los objetivos del Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas – IPSE.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos identificados en los procesos de la entidad, estas acciones son organizadas en actividades, definiendo para cada una de ellas las tareas, el responsable y sus fechas de ejecución que serán aplicadas durante la vigencia del plan.

### 1.3. Objetivos

#### 1.3.1. Objetivo general

Implementar el Sistema de Gestión de Riesgos de Seguridad y Privacidad de la Información, con el fin de minimizar, mitigar o transferir los riesgos a los cuales se expone la información, además de velar por el cumplimiento de los requerimientos legales, regulatorios y contractuales de la Entidad.

#### 1.3.2. Objetivos específicos

1. Identificar, analizar y valorar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) a los que la Entidad pueda estar expuesto.
2. Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) a los que la Entidad pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.
3. Gestionar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), de acuerdo con la Guía N°7 de MINTIC – Guía de gestión de riesgos
4. Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) de la Entidad

## 2. CONTEXTO ESTRATÉGICO

El contexto estratégico del Plan de Tratamiento de Riesgos de la Privacidad y Seguridad de la información se refiere a cómo la organización identifica y da tratamiento a los riesgos potenciales en el manejo y protección la información confidencial y privada de sus clientes, empleados y otros intereses. Esto incluye la implementación de medidas de seguridad físicas y digitales, la creación de políticas y procedimientos para el manejo de la información, y la educación y concientización de los empleados sobre los riesgos de privacidad y seguridad. Además, las organizaciones deben cumplir con las leyes y regulaciones aplicables en materia de privacidad y seguridad de la información.

En esta misma línea se pretende seguir robusteciendo este Proceso, mediante la elaboración de otros procedimientos, formatos y guías que aborden la totalidad de los servicios TI, prestados por la entidad. Por esto se hace necesario la ejecución de la herramienta de autoevaluación MSPI para establecer las brechas y establecer planes acción correspondientes.

El presente documento se elabora dando cumplimiento al Decreto 612 de 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado, entre los que menciona el plan de tratamiento de riesgos de seguridad de la información.

### 3. MARCO CONCEPTUAL

**Activo:** Cualquier cosa que tiene valor para la organización.

**Adaptabilidad:** Define los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.

**Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

**Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo aceptable.

**Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar

**Ataque:** Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

**Auditoria:** 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.

**Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad.

**Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

**Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

**Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

**Causa raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

**Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**Continuidad de la seguridad de la información:** Procesos y procedimientos para garantizar una operativa continuada de la seguridad de la información.

**Control:** Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control.

**Criterio del riesgo:** Los criterios del riesgo se basan en los objetivos de la organización y el contexto externo y el contexto interno. Los criterios de riesgo pueden derivarse de estándares, leyes, políticas y otros requisitos.

**Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

**Evento de seguridad de la información:** Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

**Fiabilidad:** Propiedad del comportamiento y de unos resultados consistentes previstos.

**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.



**Integridad:** Propiedad de la información relativa a su exactitud y completitud.

**ISO/IEC 27001:** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

**Recursos de tratamiento de información:** Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

**Requisito:** Necesidad o expectativa que es establecida, generalmente de forma implícita u obligatoria.

**Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo. La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad.

**Riesgo de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

**Riesgo de seguridad de la información:** 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).

**Riesgo inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

**Riesgo residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.

**Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

**Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

**Sistema de información:** Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información.

**Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

**Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

#### 4. MARCO NORMATIVO

Marco Normativo	Descripción
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Decreto 103 de 2015	por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1494 de 2015	Por el cual se corrigen yerros en la Ley 1712 de 2014 (Ley de Transparencia)
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 (Ley de Protección de Datos Personales), Derogado Parcialmente por el Decreto 1081 de 2015.
ISO/IEC 27001:2013:	Tecnología de la información-Técnicas de seguridad-Sistemas de Gestión de la Seguridad de la Información (SGSI)-Requisitos
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Ley estatutaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Decreto 4632 de 2011	Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
CONPES 3701 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa



Marco Normativo	Descripción
Ley 1273 de 2009	Se por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

## 5. DESCRIPCIÓN DEL PLAN

El tratamiento de riesgos de la información es el proceso de identificar, evaluar y mitigar los riesgos potenciales para la privacidad y seguridad de la información de una organización. El tratamiento de riesgos es esencial para proteger la información confidencial y cumplir con las regulaciones aplicables en materia de privacidad y seguridad de la información.



### 5.1. Establecimiento del contexto

El contexto en términos generales relaciona los aspectos externos, internos y del proceso que se deben tener en cuenta para gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) de la Entidad. A partir del contexto es posible establecer las posibles causas de los riesgos a identificar. De esta forma para la definición del contexto se seguirán las metodologías dispuestas en la entidad para lograr establecer las posibles causas y determinar la identificación de los riesgos.

### 5.2. Identificación del riesgo

Para la identificación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) de la Entidad se debe tener en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos de información, y reconocer las situaciones potenciales que causarían daño a la entidad poniendo en riesgo el logro de los objetivos establecidos.

La falta de apropiación en temas referentes a la seguridad de la información o la ausencia de controles (vulnerabilidades) puede ser aprovechadas por una amenaza causando la materialización de un riesgo (Incidente), por lo que es preciso identificar: El atributo de la triada de la información afectado (Confidencialidad, Integridad, Disponibilidad), el proceso dueño del riesgo, activo de información afectado, amenazas, vulnerabilidades y consecuencias.

Para la identificación se pueden abarcar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas.

### 5.3. Valoración del riesgo

La valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) de la Entidad se realizará acorde a la metodología para la administración de riesgos mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública.

Es así como en mesas de trabajo con los procesos se analiza el contexto, se identifican los riesgos y se realiza el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus vulnerabilidades e identificando los controles para mitigarlas. A estos controles se le identifican las variables a evaluar para el adecuado diseño de controles como son: responsable, periodicidad, propósito, cómo se realiza la actividad de control, observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo. Esta valoración se realiza de acuerdo con las tablas y metodología establecida y mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

Para los riesgos de interrupción, se indica que los controles identificados pueden ser transversales, partiendo del criterio denominado custodio del activo, puesto que cuando dicho custodio es un proceso diferente al proceso que identifica el riesgo o es un tercero, estos controles y planes de tratamiento deben establecerse de manera conjunta. El

proceso donde se identifica el riesgo aporta los niveles de probabilidad, impacto y riesgo inherente que genera la posible indisponibilidad del activo

#### **5.4. Definición y aprobación de mapas de riesgos y planes de tratamiento.**

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) de la Entidad, los líderes de los procesos deberán emitir un memorando de la aprobación de los mapas de riesgos. De igual forma en este memorando aprobarán los planes de tratamiento con las actividades requeridas que permitan mitigar aquellos riesgos cuyo nivel residual este en zona Moderada, Alta o Extrema.

#### **5.5. Materialización**

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información. Así mismo se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en el mapa de riesgos.

#### **5.6. Oportunidad de Mejora**

IPSE no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

### **6. CRONOGRAMA DE SEGUIMIENTO Y EVALUACIÓN**

Para el seguimiento y evaluación del Plan de Acción, se debe entregar trimestralmente informes con evidencias en las fechas programadas por la Oficina de Planeación.