GOBERNACIÓN DE CALDAS

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

2023

Manizales

Unidad de Sistemas

Jefatura de Gestión de la Información

Secretaría de Planeación

CONTENIDO

INTRODUCCIÓN

La información, es un recurso que como el resto de los activos, tiene valor para la Gobernación de Caldas, es crucial para su correcto desempeño dentro de la política pública y su relación con el ciudadano, y por consiguiente, debe ser debidamente protegida, ante cualquier posibilidad de alteración, mal uso, pérdida, entre muchos eventos. Las políticas de seguridad y privacidad de la información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de la misión de la entidad.

La construcción del Plan de Tratamiento de Riesgos, se enmarca dentro del Marco de Seguridad del Modelo de Seguridad y Privacidad de la Información (MSPI) liderado por el Ministerio de Tecnologías y las Comunicaciones, Decreto 1078 de 2015, Decreto 767 de 2022, la guía de Gestión del Riesgo del Departamento Administrativo de la Función Pública (DAFP) vigente y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018, adoptando las buenas prácticas, para su implementación.

Además, la Resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, tiene como objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información, la guía de gestión de riesgos de Seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y establecer los lineamientos y estándares para la estrategia de seguridad digital.

La resolución en mención precisa la necesidad de que los sujetos obligados deban adoptar las medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al Plan de Seguridad y Privacidad de la Información y así mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.

El Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, comprende una serie de actividades para la gestión de riesgo, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos de TI y por ende los objetivos de la entidad.

OBJETIVOS

- Definir y aplicar los requisitos legales y reglamentarios pertinentes para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información y los potenciales escenarios de pérdida de continuidad del negocio.
- Definir las acciones para la identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos de seguridad para proteger y preservar la integridad, confidencialidad, disponibilidad y autenticidad de la información.
- Establecer los lineamientos para la adecuada gestión de los riesgos, que den respuestas oportunas y estrategias institucionales, para reducir las vulnerabilidades ante amenazas internas y externas que puedan afectar el cumplimiento de la misión de la entidad.
- Implementar acciones, para el fortalecimiento de capacidades del recurso humano, para la identificación de los riesgos de seguridad y privacidad de la información, enfocados a la seguridad de los activos de información de la Gobernación de Caldas.

ALCANCE

Aplicar una eficiente gestión de riesgos de seguridad y privacidad de la información, que permita integrar en todos los procesos de la entidad, buenas prácticas que permitan proteger y preservar la integridad, confidencialidad, disponibilidad y autenticación de la información , con la reducción o mitigación de los riesgos de seguridad y privacidad de la información.

GLOSARIO

- Administración de Riesgos: conjunto de elementos de control que al interrelacionarse permiten a la entidad pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función.
- Análisis de Riesgo: elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo.
- Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las

actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

- Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.
- Gestión del Riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- Impacto: son las consecuencias que genera un riesgo una vez se materialice.
- Integridad: propiedad de exactitud y completitud.
- Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

MARCO REFERENCIAL

- 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.
- Decreto 1893 de 2021. Por el cual se modifica la estructura del Departamento Nacional de Planeación
- NTC ISO 31000:2018. Gestión del riesgo – Directrices
- NTC ISO 27000:2017. Se trata de la norma dedicada a Sistemas de Gestión de la Seguridad de la Información
- NTC ISO 27001:2013. Norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal.
- Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP 2020. Anexo 4.
- Decreto 767 de 2022. Política de Gobierno Digital
- Guía No.7. Seguridad y Privacidad de la Información. Gestión de Riesgos

METODOLOGÍA

Para el registro de las actividades del Plan de Tratamiento de Riesgos de Seguridad de la Información de la Gobernación de Caldas, la entidad se apoyó en la estructura contemplada en la metodología dispuestas por el DAFP en la Guía para la Administración del Riesgo - Anexo 4: Modelo Nacional de Gestión de Riesgo de seguridad de la información en entidades públicas, el diseño de controles versión 5, y los lineamientos para registro de controles del Anexo A de la ISO 27001: 2013.

Identificación de los Activos de Información: como primer paso para la identificación de riesgos de seguridad digital es necesario identificar los activos de información de la entidad. Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: Aplicaciones de la organización, Servicios web, Redes, Información física o digital, Tecnologías de Información TI, entre otros; además permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios), así la entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

- Identificación de los Riesgo: identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su

objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Para identificar los riesgos inherentes a la seguridad de la información, se enmarcan en 3 riesgos: pérdida de la confidencialidad, pérdida de la integridad y pérdida de disponibilidad.

- Identificación y evaluación de los controles existentes: una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios. Para esta acción, se toma como referencia el Anexo A de la Norma ISO/IEC 27001:2013.

- Tratamiento del Riesgo: una vez se han identificado los riesgos, la entidad debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos previamente en la Política de Administración de Riesgos de la entidad. El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, la entidad tiene en cuenta las opciones planteadas en la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" del DAFP: Evitar, aceptar, compartir o mitigar el riesgo.

Los planes de tratamiento de riesgos y los indicadores para medir la eficacia o la efectividad se deberán generar como lo indica el Esquema 9. Consolidación

de los Planes de Tratamiento de Riesgos, de la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" emitida por el DAFP.

- Monitoreo y revisión : La entidad, a través de las Tres Líneas de defensa definidas en el MIPG, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:
  - Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
  - Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
  - Realizar monitoreo de los riesgos y controles tecnológicos.
  - Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
  - Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
  - Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

- Mejoramiento continuo de la gestión del riesgo de seguridad digital : se definen las acciones para mejorar continuamente la gestión de riesgos de seguridad digital de la siguiente forma:
  - Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizados.

- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Item	Actividad	Tarea	Responsable	Fecha de Inicio	Fecha Fin
1	Identificación de los Activos de información	Actualizar los activos de información	Gestión Documental Unidad de Sistemas	1-feb-23	28-abr-23
2	Adopción de Lineamientos inherentes a la gestión del riesgo	Crear y/o actualizar la política, metodología y procedimiento de gestión del riesgo	Jefatura Gestión de la Información Unidad de Sistemas	1-feb-23	28-abr-23
3	Identificación y valoración de los Riesgos de Seguridad y Privacidad de la Información	Identificación y valoración de nuevos riesgos de seguridad de la información	Jefatura Gestión de la Información Unidad de Sistemas	1-mar-23	28-abr-23
		Actualizar los riesgos de seguridad de la información ya registrados	Jefatura Gestión de la Información Unidad de Sistemas	1-mar-23	28-abr-23
4	Identificación y evaluación de los controles existentes	Implementación de los controles adoptados	Unidad de Sistemas	1-may-23	31-dic-23
5	Tratamiento de los Riesgos	Implementación de los planes de tratamiento de riesgos	Unidad de Sistemas	1-may-23	31-dic-23
6	Monitoreo y Revisión	Realizar seguimiento al plan de acción en la etapa de implementación y finalización	Undidad de Sistemas	1-may-23	31-dic-23
7	Socialización del mapa de riesgos	Presentar un informe con el resultado del plan de acción implementado	Unidad de Sistemas	1-jun-23	30-jun-23
8	Mejoramiento continuo de la gestión del riesgo de seguridad digital	Registro planes de mejora acorde con los resultados obtenidos	Unidad de Sistemas	1-may-23	31-dic-23
		Implementación acciones plan de mejora	Unidad de Sistemas	1-may-23	31-dic-23

Unidad de Sistemas

Jefatura de Gestión de la Información

Secretaría de Planeación

Control de Cambios				
Cambios Realizados	**Fecha**	**Versión**	**Preparado por**	**Aprobado por**
Creación documento	01/02/2021	01	Jefatura Gestión de la Información	Jefatura Gestión de la Información
Actualización	17/01/2023	02	Unidad de Sistemas	Jefatura Gestión de la Información