República de Colombia

Gobernación de Santander

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL 2019-2021

DIDIER ALBERTO TAVERA AMADO
Gobernador de Santander

JULIO CÉSAR GÓMEZ SUÁREZ
Secretario de las TIC

Bucaramanga, Octubre de 2019

Título:	Plan de Tratamiento de Riesgos de Seguridad Digital 2019-2021				
Fecha Elaboración	Octubre de 2019				
Formato	Documento Texto	Lenguaje:	Español		
Dependencia:	Secretaría de Las Tecnologías de la Información y Comunicación				
Código:	AP-TIC-PL-03	Versión:	0	Estado:	Terminado
Autor (es):	Secretaría TIC de Santander				
Otros Colaboradores:	Jhon Jairo Jiménez Álvarez: c.jhjimenez@santander.gov.co Ingeniero de Sistemas - M.Sc. en Tecnologías de la Información y las Comunicaciones Yoham Efrén Rojas González: c.yrojas@santander.gov.co Ingeniero Electrónico – Especialista en Telecomunicaciones Juan Sebastián Rodríguez Mejía: c.jurodriguez@santander.gov.co Ingeniero Industrial Leonardo Fabio Pérez Vega: c.lperez@santander.gov.co Ingeniero Industrial				
Revisó	Ing., Julio Cesar Gómez Suárez Secretario de las TIC				
Aprobó:	Comité Institucional de Gestión y Desempeño				
Ubicación:	Secretaría de Tecnologías de la Información y la Comunicación SETIC – Calle 48 N° 27ª – 48 Santander - Bucaramanga Correo: setic@santander.gov.co Facebook: Setic Santander Twitter: @TICSantander				

Tabla de Contenido

Lista de Tablas

Lista de Ilustraciones

1. INTRODUCCIÓN

Teniendo en cuenta la necesidad de Administrar de manera optimizada los riesgos de las Instituciones Públicas, el Gobierno departamental, ha establecido el siguiente plan para la administración del riesgo y diseño de controles de seguridad digital de acuerdo con los lineamientos establecidos por el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y Comunicaciones.

La gestión de riesgos de seguridad digital establece procesos, procedimientos y actividades encaminados a lograr un equilibrio entre la prestación de servicios y los riesgos asociados a los activos de información que dan apoyo y soporte en el desarrollo de la misionalidad de la entidad. Por lo tanto se deben implementar los controles necesarios para dar un adecuado tratamiento a los riesgos, generando una estrategia de seguridad digital efectiva que controle y administre la materialización de eventos o incidentes, mitigando los impactos adversos o considerables al interior de la entidad.

El presente Plan de Gestión de Riesgos de Seguridad Digital inicia con la definición del contexto de los riesgos de seguridad digital a los que está expuesta la entidad dando cubrimiento a los procesos estratégicos, misionales, de control y seguimiento, y de apoyo, y concluye con el plan de acción mediante el cual se realizará el tratamiento, monitoreo y revisión de los riesgos de seguridad digital identificados.

2. OBJETIVO GENERAL

Establecer un marco de gestión de riesgos de seguridad digital a través del cual se mitiguen las vulnerabilidades y amenazas asociadas a los activos de información, con el fin de lograr niveles de aceptación razonable del riesgo en relación con los atributos de disponibilidad, integridad y confidencialidad de la información de la entidad.

2.1. Objetivos Específicos

- Establecer lineamientos específicos para la identificación de los riesgos de Seguridad Digital través del establecimiento del contexto de identificación.
- Evaluar y analizar los riesgos de seguridad digital relacionados a los activos de información para facilitar el desarrollo de la misionalidad de la Gobernación de Santander.
- Identificar las amenazas e impactos de seguridad digital asociadas a los procesos de la entidad.
- Identificar e implementar controles que atiendan la gestión de riesgos y facilite la toma de decisiones sobre el riesgo residual.
- Definir el plan de tratamiento del riesgo residual de la entidad.

3. ALCANCE

El presente plan es aplicable a todos los procesos que conforman el Sistema Integrado de Gestión de la Gobernación de Santander y a todas las actividades realizadas por los servidores públicos durante el ejercicio de sus funciones contemplando riesgos de seguridad digital y privacidad de la información.

4. DEFINICIONES O SIGLAS

Para la adecuada gestión de riesgos de seguridad digital se debe manejar con propiedad los siguientes términos:

Activo: [Según **ISO 27000**]: 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.

Amenaza: [Según **ISO 27000**]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis del riesgo: [NTC ISO 31000:2011]: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Apetito de riesgo: Es el nivel máximo de riesgo que la entidad está dispuesta a asumir.

Consecuencia: [NTC ISO 31000:2011]: Resultado o impacto de un evento que afecta a los objetivos.

Controles: [Según ISO 27000]: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

CSIRT: Equipo de Respuesta a Incidentes de Seguridad Informática

Criterios del riesgo: [Según NTC ISO 31000:2011]: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

Evaluación del riesgo: [Según NTC ISO 31000:2011]: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Identificación del riesgo: [Según NTC ISO 31000:2011]: Proceso para encontrar, reconocer y describir el riesgo.

Impacto: [Según ISO 27000]: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Inventario de activos: [Según ISO 27000.ES]: Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.

Nivel de riesgo: [Según NTC ISO 31000:2011]: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad.

Perfil del riesgo: [Según NTC ISO 31000:2011]: Descripción de cualquier conjunto de riesgos.

Política: [Según ISO/IEC 27000:2016]: Intenciones y dirección de una organización como las expresa formalmente su alta dirección.

Política: para la gestión del riesgo [Según NTC ISO 31000:2011]: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

Reducción del riesgo: [Según NTC ISO 31000:2011]: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo.

Riesgo: [Según ISO 27000]: 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.

Riesgo Residual: [Según ISO 27000]: El riesgo que permanece tras el tratamiento del riesgo.

Vulnerabilidad: [Según ISO 27000]: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La Secretaría de Tecnologías de la Información y Las Comunicaciones de la Gobernación de Santander siguiendo los lineamiento trazados por el Gobierno Nacional con lo expuesto en la Ley de transparencia 1712 de 2014, la Estrategia Gobierno en línea y la Política de Gobierno Digital. Establece un **PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL** en el cual se identifiquen las amenazas, las vulnerabilidades, el impacto y el nivel de riesgo asociados a los activos de información sin importar el nivel de criticidad que tienen para la entidad.

En la gestión de riesgos de seguridad digital resulta importante lograr una aceptación de los riesgos con base en las posibles consecuencias de afectación; establecer una estrategia de mitigación adecuada que logre un entendimiento y aceptación del riesgo residual así como de los recursos empleados en relación costo beneficio con el fin de emplear medidas para salvaguardar, proteger y custodiar los activos de información de las aplicaciones, servicios tecnológicos, bases de datos, redes de comunicaciones, equipos de cómputo y documentos físicos garantizando la disponibilidad, confidencialidad e integridad de la información. Por consiguiente, resulta indispensable definir actividades que de manera articulada permitan implementar medidas de control que ayuden a la prevención, contención y mitigación de amenazas a las que se encuentran expuestos los activos de información de la entidad por medio de una metodología descrita a continuación:

5.1. Fase de Identificación

5.1.1. Establecimiento del Contexto

Consiste en la definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC-ISO 31000). A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.

Para identificar estos parámetros es de vital importancia en primera medida realizar un análisis de los objetivos estratégicos y metas de la Gobernación de Santander, seguido de este el establecimiento de un contexto interno, externo y por procesos para así lograr identificar los riesgos de seguridad digital presentes en cada una de las actividades de la entidad y establecer controles que permitan mitigación o reducir su impacto.

Contexto Externo: Para determinar los factores del contexto externo que afecten la seguridad digital de la gobernación de Santander se implementará la metodología **PESTAL**, la cual permite evaluar factores Políticos, Económicos, Sociales, Tecnológicos, Legales y Ambientales. Es por esto que se utilizará el siguiente formato para su documentación e identificación de riesgos potenciales inherentes a los factores externos identificados.

Tabla 1. Formato de identificación de riesgos inherentes a Factores Externos

Factor	Amenaza	Descripción del Riesgo
Político	Cambios De Gobierno, Legislación, Políticas Públicas, Regulación.	
Económico	Disponibilidad De Capital, Liquidez, Mercados Financieros, Desempleo, Competencia.	
Social	Demografía, Responsabilidad Social, Orden Público.	
Tecnológico	Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.	

Ambiental	Emisiones y Residuos, Energía, Catástrofes Naturales, Desarrollo Sostenible.	
Legal	Normatividad Externa (Leyes, Decretos, Ordenanzas y Acuerdos).	

Contexto Interno: La secretaría de Tecnologías de la Información y las comunicaciones dentro de su contexto interno determinará las características o aspectos del ambiente tales como son su estructura organizacional, funciones y responsabilidades, políticas, objetivos, estrategias implementadas, recursos (económicos, personas, procesos, sistemas, tecnología, información), relaciones con las partes involucradas y cultura organizacional para determinar en ellos factores que puedan afectar la seguridad digital y que sean factores de riesgo inherente para la Gobernación de Santander. Para esto se utilizará un formato similar al utilizado para determinar el contexto externo para así clasificar las debilidades encontradas.

Tabla 2. Formato de Identificación de Riesgos Inherentes a Factores Internos.

Factor	Debilidad	Descripción del Riesgo
Financieros	Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.	
Personal	Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.	
Procesos	Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.	
Tecnología	Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.	
Estratégicos	direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo	
Comunicación interna	Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.	

Contexto del Proceso: Igualmente, es necesario determinar los factores inherentes al desarrollo de los procesos que afectan la seguridad digital de la gobernación de Santander, es por esto que se analizaran factores como el diseño de los procesos, las interacciones con otros procesos, transversalidad, procedimientos asociados,

responsable del proceso, Comunicación entre procesos y los activos de seguridad digital del proceso. Al igual que con los factores externos e internos también se construirá un formato que permita su documentación y administración, para eso se utilizará el siguiente formato.

Tabla 3. Formato de Identificación de Riesgos Inherentes al Contexto del Proceso.

Factor	Debilidad	Descripción del Riesgo
Diseño del proceso	Claridad en la descripción del alcance y objetivo del proceso.	
Interacciones con otros procesos	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.	
Transversalidad	Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.	
Procedimientos asociados	Pertinencia en los procedimientos que desarrollan los procesos.	
Responsables del proceso	Grado de autoridad y responsabilidad de los funcionarios frente al proceso.	
Comunicación entre los procesos	Efectividad en los flujos de información determinados en la interacción de los procesos.	
Activos de seguridad digital del proceso	Información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso.	

5.1.2. Identificación de partes interesadas y procesos donde se aplique la gestión de seguridad digital

La entidad debe identificar las partes interesadas que afecten o puedan verse afectadas en el entorno digital. De acuerdo con el (CONPES 3854, pág. 29) y en general con los sistemas de gestión mundialmente reconocidos establecen que las múltiples partes interesadas incluyen: el Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la fuerza pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia, la sociedad civil, entes de control a nivel nacional tipo contralorías y personerías, entre otras; y a nivel internacional, entidades como el Banco Interamericano de Desarrollo (BID) o el Banco Mundial (BM), que pueden tener un mayor interés dada la financiación de programas sociales a través de entidades públicas como ministerios o entidades del sector público, entre otros; quienes dependen del entorno digital para todas o algunas de sus actividades económicas y sociales, y quienes pueden ejercer distintos roles y tener diferentes responsabilidades.

De igual forma, como parte de la fase de planificación, se hace necesaria la identificación de los procesos en los cuales se desarrolla la gestión de riesgos de seguridad digital.

Nota: para implementar esta actividad, se establece el numeral 4.1.3. Identificación de las partes interesadas, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

5.1.3. Identificación de activos

Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones **funcionen y consigan los objetivos** que se han propuesto por la alta dirección. Para el caso de la gobernación de Santander encontramos diferentes activos de información entre los que se encuentran documentos, bases de datos, software, hardware y aplicaciones entre otros.

De esta manera se puede determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, unos archivos, servidores web o aplicaciones claves 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.

La entidad debe identificar todos los activos de información (se incluyen los que corresponden a las ICC) y se clasifican de acuerdo con la normatividad vigente y aplicable (por ejemplo, para entidades públicas se deben tener en cuenta la ley 1712 de 2014 y la ley 1581 de 2012), que determinan la importancia del activo para la entidad e identifican el nivel de criticidad.

Es importante resaltar que si la entidad presta servicios esenciales, *"los necesarios para el mantenimiento de las funciones sociales básicas, salud, seguridad, bienestar social y económico de los ciudadanos o el funcionamiento de las instituciones del Estado y las administraciones públicas"*[1], se deben establecer cuáles de los servicios esenciales hacen parte de la infraestructura crítica nacional, de acuerdo con los criterios de criticidad definidos por el CCOC, en la *"Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia Primera Edición"*[2] y en ese caso, deben reportarse al CCOC y, posteriormente, a la aplicación del proceso de la GRSD. Es decir, se deben reportar las ICC identificadas en la entidad y también los riesgos asociados a estas infraestructuras críticas.

---

[1] Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia, primera edición CCOC.

[2] Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia, primera edición CCOC.

Nota: para implementar esta actividad, se establece el numeral 4.2.1 Identificación de activos de información, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

Es por esto, que una correcta identificación de activos de información es de vital importancia a la hora de administrar los riesgos de seguridad digital presentes en los diferentes procesos de la arquitectura de la Gobernación de Santander. Para este plan se tiene establecido realizar un inventario de activos de información presentes en la gobernación de Santander de la siguiente manera:

- Realizar el inventario de documentos o bases de datos consideradas activo de información en cada uno de los 12 procesos del Mapa de procesos del sistema integrado de gestión de calidad, analizando cada una de las direcciones o coordinaciones del proceso según sea el caso.

- Realizar un inventario de software, hardware y aplicaciones utilizados en la gobernación de Santander en los procesos estratégicos, misionales, de apoyo o de control y seguimiento.

Adicionalmente, se debe establecer la criticidad de cada uno de los activos encontrados en los inventarios realizados con el fin de establecer controles efectivos, eficientes y eficaces a la hora de administrar los riesgos de los mismos.

5.1.4. Definición de Roles

Según los principios generales, la gestión del riesgo es una actividad que se realiza en toda la organización. Por lo tanto, la dirección es responsable de apoyar el proceso en su totalidad. Esto incluye la planificación estratégica, la gestión de proyectos y la gestión de cambio, entre otros.

Por otra parte, la GRSD debe ser compromiso de cada uno de los integrantes de la entidad, no obstante, la gestión es responsabilidad de los líderes de proceso, los cuales son los propietarios de los riesgos. Igualmente, la entidad al aplicar el MGRSD debe definir claramente quién se hará cargo de la coordinación, seguimiento, reporte de los avances, logros e inconvenientes relacionados con la gestión de los riesgos de seguridad digital.

Nota: para implementar esta actividad, se establece el numeral 4.1.6. Definición de roles y responsabilidades, dentro de las guías de orientación para la gestión de riesgos de seguridad digital, de acuerdo con el tipo de entidad al que pertenece (Gobierno nacional, entes territoriales y sector público, mixto y privado, así como fuerza pública).

5.1.5. Identificación de los riesgos

Identificar los riesgos inherentes de seguridad digital Como lo indica el Paso 2 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, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- 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.

A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

Identificación de Amenazas: Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

- Deliberadas (D), fortuito (F) o ambientales (A).

Tabla 4. Amenazas Comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D,F
	Mal funcionamiento del equipo	D,F
	Saturación del sistema de información	D,F
	Mal funcionamiento del software	D,F
	Incumplimiento en el mantenimiento del sistema de información	D,F
Acciones no autorizadas	Uso no autorizado del equipo	D,F
	Copia fraudulenta del software	D,F
Compromiso de las funciones	Error en el uso o abuso de derechos	D,F
	Falsificación de derechos	D

Fuente: ISO/IEC 27005:2009

Importante: La entidad pública puede decidir si realiza la gestión de riesgos en todos los activos identificados en este punto o si desea hacerlo a los activos más críticos. Esta decisión debe estar debidamente formalizada en el procedimiento de gestión de activos que solicita el Modelo de Seguridad y Privacidad de la Información. Adicionalmente, debe quedar explícita en la Política de Administración de Riesgos de la entidad pública, debidamente aprobada por el Comité Institucional de Coordinación de Control Interno.

- Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Tabla 5. Amenazas dirigidas por el hombre

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información	Crimen por computador Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema DDoS Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de información
Intrusos (empleados con Curiosidad Asalto a un empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ganancia monetaria	Asalto a un empleado Chantaje

Fuente: ISO/IEC 27005:2009

Identificación de vulnerabilidades: la entidad pública puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Tabla 6. Vulnerabilidades Comunes

Tipo	Vulnerabilidades
	Mantenimiento insuficiente

Tipo	Vulnerabilidades
Hardware	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros

Fuente: ISO/IEC 27005:2009

La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una

vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Identificación del riesgo inherente de seguridad digital: Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.

Adicionalmente, se debe identificar el dueño del riesgo, es decir, “quien tiene que rendir cuentas sobre el riesgo o quien tiene la autoridad para gestionar el riesgo”.

La identificación de riesgos, amenazas y vulnerabilidades puede ser realizada a través de diferentes metodologías. Como ejemplo, se citan las siguientes:

- **Lluvia de ideas:** mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas asociadas al manejo de la información digital y los activos de información se pueden presentar o casos ocurridos que los participantes conozcan que se hayan dado en la entidad pública o en el sector. Deben existir un orden de la sesión, un líder y personas que ayuden con la captura de las memorias.

- **Juicio de expertos:** a través de este esquema se reúnen las personas con mayor conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad digital se pueden presentar. Para emplear esta técnica, se requiere disponer de una agenda con un orden de temas, establecer reglas claras y contar con la participación de un orientador o moderador, así como personas que tomen notas de los principales conceptos expuestos. Al finalizar, se retoman los principales riesgos identificados y se procede a hacer una valoración

- **Análisis de escenarios:** en este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse: explosión de un pozo, sobrecarga de un nodo, pérdida de control de una unidad operada remotamente; y con base en estas posibilidades, se determina qué puede llegar a suceder, desde la perspectiva digital, a los activos de información y las consecuencias de la afectación.

- **Otras técnicas que pueden ser empleadas son:** entrevistas estructuradas, encuestas o listas de chequeo.

5.1.6. Identificación y evaluación de controles existentes

Como lo indica la Guía de DAFP, arriba mencionada, 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 determinar si existen uno o varios controles asociados a los riesgos inherentes identificados se pueden consultar la sección **4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA** (Tomados del Anexo A de la Norma ISO/IEC

27001:2013) como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad digital que están enunciados en dicho anexo.

6. ANÁLISIS DE RIESGOS

Se realiza la identificación de causas, vulnerabilidades, amenazas (identificación, descripción, tipo), consecuencias y se determina la clase de riesgo (probabilidad e impacto), todo esto asociado a aquellos eventos o situaciones que afecten los activos de información que pueden entorpecer el normal desarrollo de los procesos.

6.1. Análisis De Causas

Para el análisis de causas se deben establecer claramente cada una de las actividades desarrolladas para el cumplimiento de los objetivos estratégicos y las desarrolladas al interior de cada proceso; se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se deben tener en cuenta al identificar las causas que originan la materialización de los riesgos.

Para identificar factores externos se puede emplear el acrónimo PESTAL, es decir, factores: políticos, económicos, sociales, tecnológicos, ambientales, y legales. Para los riesgos de seguridad digital, se tomará como base el análisis realizado al interior de cada proceso.

6.2. Determinar Probabilidad

Por PROBABILIDAD se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.

Bajo el criterio de **FRECUENCIA** se analizan el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

Bajo el criterio de **FACTIBILIDAD** se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que se dé.

6.2.1. Análisis de la probabilidad

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Posteriormente, se califica el nivel de probabilidad en términos de factibilidad y se utiliza una matriz para la calificación.

Tabla 7. Criterios para calificar la probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

En caso de que la Gobernación no cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, los integrantes del equipo de trabajo deben calificar en privado el nivel de probabilidad en términos de factibilidad, utilizando la siguiente matriz de priorización de probabilidad.

Tabla 8. Matriz de priorización de la Probabilidad.

N.°	RIESGO	P1	P1	P1	P1	P1	P1	TOT	PROM	
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	Se espera que el evento ocurra en la mayoría de las circunstancias.								
2	Otros riesgos identificados	Es viable que el evento ocurra en la mayoría de las circunstancias.								
3	Otros riesgos	El evento podrá ocurrir en algún momento.								
Convenciones: N.°**: número consecutivo del riesgo -** P1**: participante 1 P… -** Tot**: total puntaje -** Prom**.: promedio**										

El análisis de frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre el evento o riesgo identificado. En caso de no contar con datos históricos, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos.

6.3. Determinar Consecuencias O Nivel De Impacto

Por IMPACTO se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Se tienen en cuenta las consecuencias potenciales establecidas en el paso 2 de identificación del riesgo, 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.

Para su determinación se utiliza la tabla de niveles de impacto establecida en la Política de Riesgos en la organización que puede ser catastrófico, mayor, moderado, menor e insignificante. Cada entidad deberá adaptar los criterios de acuerdo con su complejidad.

Tabla 9. Criterios para calificar el impacto

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
MODERADO	3	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recupera-ción.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
			debido al interés particular de los empleados y terceros.
MAYOR	4	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
CATÁSTRÓFICO	5	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. 2017

- Cada entidad deberá adaptar los criterios a su realidad. El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

- Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

- La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en

los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

- La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

- La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

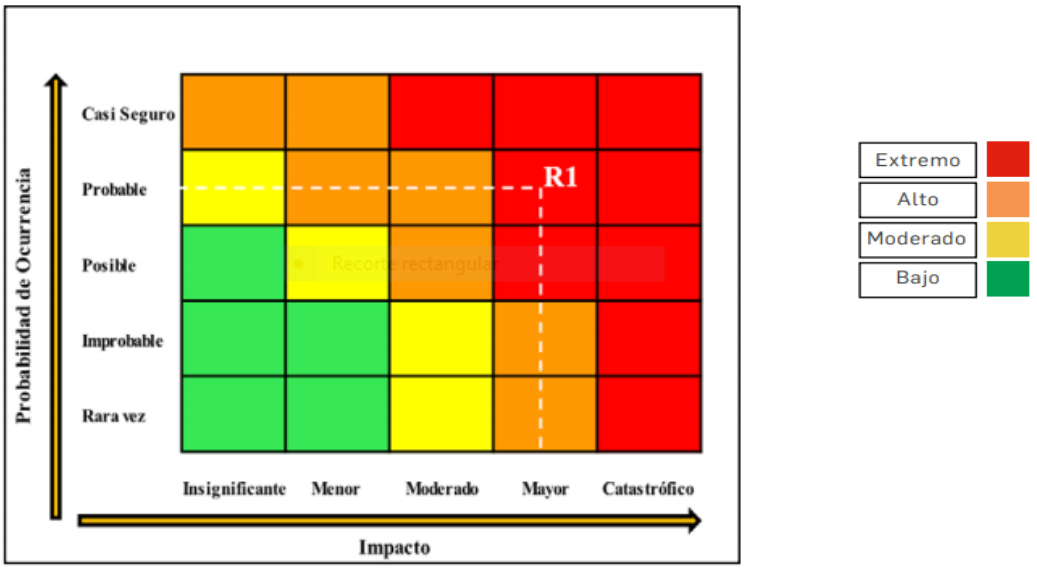
6.3.1. Análisis de impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo. Para el ejemplo que venimos explicando, el impacto fue identificado como mayor por cuanto genera interrupción de las operaciones por más de dos días. El nivel del impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

6.3.2. Mapa de calor

Se toma la calificación de probabilidad resultante de la tabla “Matriz de priorización de probabilidad”, para este ejemplo se tomará la probabilidad de ocurrencia en “probable” y la calificación de impacto en “mayor”, ubique la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, establezca el punto de intersección de las dos y este punto corresponderá al nivel de riesgo, que para el ejemplo es nivel extremo – color rojo (R1), Así se podrá determinar el riesgo inherente.

Ilustración 1. Mapa de Calor para Determinar el Riesgo Inherente.



Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. 2017.

7. EVALUACIÓN DEL RIESGO

7.1. Riesgo antes y después de controles

Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice

Para la valoración del riesgo antes y después de controles, la guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, indica los siguientes pasos:

- **Riesgo antes de controles:** se identifican los riesgos inherentes o subyacentes que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso. En este punto se ubica el riesgo dentro del mapa de calor, para conocer el grado en el que se encuentra inicialmente.
- **Causas o fallas:** Se identifican las causas o fallas que pueden dar origen a la materialización del riesgo.
- **Controles:** Para cada causa se identifica el control o controles.
- **Riesgo después de controles:** Evaluar si los controles están bien diseñados para mitigar el riesgo y si estos se ejecutan como fueron diseñados. Una vez se identifican los controles, se ubica nuevamente dentro del mapa de calor para conocer el grado de mitigación del mismo.

Para cada causa debe existir un control. Las causas se deben trabajar de manera separada (no se deben combinar en una misma columna o renglón). Un control puede ser tan eficiente

que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.

7.2. Valoración de los controles – Diseño de controles

Antes de valorar los controles es necesario conocer cómo se diseña un control. Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo.

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:

- Debe tener definido el responsable de llevar a cabo la actividad de control.
- Debe tener una periodicidad definida para su ejecución.
- Debe indicar cuál es el propósito del control.
- Debe establecer el cómo se realiza la actividad de control.
- Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
- Debe dejar evidencia de la ejecución del control.

Las acciones de tratamiento se agrupan en:

- Disminuir la probabilidad: acciones encaminadas a gestionar las causas del riesgo
- Disminuir el impacto: acciones encaminadas a disminuir las consecuencias del riesgo

Al momento de definir si un control o controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables: responsable, periodicidad, propósito, cómo se realiza, qué pasa con las observaciones o desviaciones, evidencia de la ejecución del control.

7.2.1. Valoración de los controles

Para la adecuada mitigación de los riesgos, no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

Análisis y evaluación de los controles para la mitigación de los riesgos se puede realizar según los criterios de evaluación, de acuerdo con las 6 variables establecidas (responsable, periodicidad, propósito, cómo se realiza, qué pasa con las observaciones o desviaciones, evidencia de la ejecución del control), identificando aspectos a evaluar en el diseño del control, y opciones de respuesta.

Posteriormente se asignan un peso o participación para cada una de las variables en el diseño del control para la mitigación del riesgo.

7.2.2. Resultados de la evaluación del diseño del control

El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables, para que un control se evalúe como bien diseñado

7.2.3. Resultados de la evaluación de la ejecución del control

Aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurarse por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se confirma con las actividades de evaluación realizadas por auditoría interna o control interno.

7.2.4. Análisis y evaluación de los controles para la mitigación de los riesgos

Dado que la calificación de riesgos inherentes y residuales se realiza al riesgo y no a cada causa, hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto sí ayudan al tratamiento de los riesgos, considerando tanto el diseño, ejecución individual y promedio de los controles. En la evaluación del diseño y ejecución de los controles, las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, por lo que siempre la calificación de la solidez de cada control, asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil.

7.2.5. Solidez del conjunto de controles para la adecuada mitigación del riesgo

Dado que un riesgo puede tener varias causas, a su vez varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo.

La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo, calificando la solidez del conjunto de controles en: fuerte, Moderado y Débil.

7.3. Nivel de riesgo (riesgo residual)

7.3.1. Desplazamiento del riesgo inherente para calcular el riesgo residual.

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual.

Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

7.3.2. Resultados del mapa de riesgo residual.

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de riesgo residual (después de los controles).

8. TRATAMIENTO DEL RIESGO

Una vez se han identificado los riesgos, la entidad pública 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 Institucional. El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, la entidad pública puede tener 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.

9. MONITOREO Y REVISIÓN

La entidad pública a través de las Tres Líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, Componente Actividades de control, 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.

Nota: Una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la entidad pública debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el último nivel de riesgo residual.

En esta fase se deben evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles propuestos, de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad pública. Así mismo, también deberán tenerse en cuenta los incidentes de seguridad digital que hayan afectado a la entidad y también las métricas o indicadores definidos para hacer seguimiento a las

medidas de seguridad implementadas. Todo lo anterior contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la línea estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y las partes interesadas.

9.1. Registro y reporte de incidentes de seguridad digital

Es importante que la entidad pública cuente con el registro de los incidentes de seguridad digital que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.
Igualmente se deben realizar el reporte de incidentes de seguridad de la información a los entes de control, reguladores, superintendencias, y demás autoridades en la materia, conforme lo estipulan los entes o las buenas prácticas establecidas en seguridad digital.

9.2. Reporte de la gestión del riesgo de seguridad digital

El responsable de seguridad digital debería reportar periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:

Ilustración 2. Reportes de información por parte de la entidad.

REPORTE

- Matriz de los riesgos identificados de seguridad digital.
- Listado de activos críticos TI/TO y listado de ICC.
- Reporte de criticidad sobre impacto de la organización.
- Plan de tratamiento de riesgos.
- Reporte de evolución de riesgos y modificación del apetito de riesgo.
- Cantidad de riesgos por fuera de la tolerancia del riesgo identificados de acuerdo con la periodicidad de evaluación realizada.
- Impacto económico que podría presentarse frente a la materialización de los riesgos.

PERIODICIDAD

- Periódicamente por parte de las Entidades u organizaciones Que han adaptado el modelo respectivo.
- Cuando ocurra un cambio organizacional o de los procesos de la organización que genere un impacto en las operaciones o pueda afectar los riesgos ya identificados anteriormente. En este caso debe realizarse una nueva evaluación de los riesgos y reportar los resultados a la entidad de control.
- Cuando se incluya un nuevo proceso dentro del alcance de la gestión de riesgos de seguridad digital de la organización. En este caso se debe realizar una nueva evaluación de riesgos y reportar los resultados a la Entidad de control.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

9.3. Reporte de la gestión del riesgo de seguridad digital a autoridades o entidades especiales.

Una vez la entidad pública obtenga los resultados de la gestión de riesgos de seguridad digital, se debería consolidar información (previamente obtenida con la aplicación del modelo) con el fin de reportarla a futuro a las autoridades o instancias encargadas del tema y que el Gobierno defina.

La finalidad del reporte de esta información es que el Gobierno Nacional pueda identificar posibles oportunidades para la generación de política pública, generación de capacidades o asignación de recursos que permita ayudar a la mejora de la seguridad digital.
Información por consolidar para generar el reporte de información:

Se propone que las entidades públicas consoliden la siguiente información puntual para poder llevar a cabo el reporte respectivo:

- Riesgos con nivel crítico
- Amenazas críticas
- Vulnerabilidades críticas
- Tipos de Activos afectados por los riesgos críticos (incluyendo servicios digitales o que delimitan con internet)
- Planes de tratamiento propuestos para la mitigación y si han sido ejecutados
- Servicios digitales críticos en la entidad pública (Servicios o trámites para los ciudadanos o sistemas de información críticos para la entidad).

Esta información tiene por objetivo permitir la construcción de un panorama de riesgos de seguridad digital de todo el país, para poder tomar decisiones estratégicas para la construcción de política pública, generación de capacidades o planes de acción con base a la información que pueda analizarse.

- **Reportes relacionados con Infraestructuras Críticas Cibernéticas, cuando aplique:**

Las infraestructuras críticas cibernéticas -ICC- que hayan sido identificadas deberían reportarse a las autoridades o instancias encargadas del tema en el Gobierno nacional.

Nota: Es importante indicar que los reportes de riesgos de seguridad digital a las entidades de gobierno no implicarían o significarían el traslado de la responsabilidad sobre los riesgos o su tratamiento.

9.4. Auditorías internas y externas

Le corresponde a las Unidades de Control Interno (tercera línea de defensa), realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo de seguridad digital en la entidad pública, catalogándola como una unidad auditable más dentro de su Universo de Auditoría, conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno de la entidad.

9.5. Medición del desempeño

La entidad pública debe utilizar medidas de desempeño (indicadores) para la gestión de los riesgos de seguridad digital, las cuales deben reflejar el cumplimiento de los objetivos propuestos. Estas deben ser evaluadas periódicamente alineadas con la revisión por la línea estratégica.

9.5.1. Indicadores - gestión del riesgo de seguridad digital

Igualmente, en el caso de los riesgos de seguridad digital, se deben generar indicadores, para medir la gestión realizada, en esencia en cuanto a la eficacia y la efectividad de los planes de tratamiento implementados. La entidad debería definir como mínimo 2 indicadores POR PROCESO de la siguiente manera:

- 1 indicador de eficacia, que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada PROCESO de la entidad.
- 1 indicador de efectividad, para cada riesgo o la suma de todos los riesgos de seguridad digital (pérdida de confidencialidad, de integridad, de disponibilidad).

10. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DEL RIESGO

Una vez se haga la identificación de los Riesgos su análisis y establecimiento de controles, se deben establecer líneas de defensa o acciones a seguir, en caso de materialización de cada uno de los riesgos identificados.
Adicionalmente, se debe establecer un procedimiento que permita reevaluar los riesgos para establecer controles que permitan la no materialización de un riesgo futuro.

11. MEJORAMIENTO CONTINUO DE LA GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

La entidad pública debe garantizar la mejora continua de la gestión de riesgos de seguridad digital, por lo tanto, debe establecer que cuando existan hallazgos, falencias o incidentes de seguridad digital se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse. Deben definirse 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 realizadas, otras auditorías e informes de los entes de control.

- 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.

Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

12. PLAN DE COMUNICACIONES

Participan todos los procesos e involucran a todos los colaboradores para el levantamiento de los mapas de riesgo, contando con el aporte de los colaboradores con mayor experticia tanto para la identificación como para el tratamiento de riesgos. Cuando se identifica un riesgo el Instituto suministra, comparte u obtiene información a través de un diálogo con las partes involucradas con respecto a la gestión del riesgo. La información está relacionada con la existencia, la naturaleza, la forma, la probabilidad, el significado, la evaluación, la aceptabilidad y el tratamiento de la Gestión de riesgo.

13. CRONOGRAMA

Tabla 10. Hoja de Ruta de Implementación del Plan de Gestión de Riesgos de Seguridad Digital.

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
1	Actualización metodología de Riesgos de Seguridad Digital.	Enero 2020	Marzo 2020	Equipo Sistemas de Gestión de Seguridad de la Información	Matriz de riesgos
2	Información sobre la evaluación de riesgos de Seguridad Digital	Marzo 2020	Mayo 2020	Equipo SGSI	Comunicaciones internas / Correo electrónico
3	Identificación y Análisis de Riesgos Seguridad Digital	Febrero 2020	Diciembre 2020	Todas las áreas y acompañamiento de Equipo SGSI	Matriz de riesgos
4	Publicación de riesgos de Seguridad Digital.	Enero 2021	Enero 2021	Equipo SGSI	Link de transparencia

5	Tratamiento de Riesgos de Seguridad Digital	Febrero 2021	Diciembre 2021	Todas las áreas y acompañamiento de Equipo SGSI	Actas de reunión / correos electrónicos
6	Información de seguridad Seguimiento de Riesgos y Revisión - Informe	Junio 2021	Diciembre 2021	Equipo SGSI – Oficina de Control Interno	Informe de riesgos

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**REVISÓ**	**APROBÓ**
0	03/10/2019	Creación del Documento	Secretaría de Tecnologías de la información y comunicaciones Dirección de Sistemas Integrados de Gestión.	Comité Institucional de Gestión y Desempeño