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

VIGENCIA 2024

TABLA DE CONTENIDO

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

1. INTRODUCCIÓN

En el contexto de la transformación digital que ha venido experimentando el mundo entero, y por consiguiente Colombia y sus entidades, hay un sin número de riesgos de seguridad y privacidad de la información que amenazan a las entidades con materializarse y que de ser así impactarían negativamente el funcionamiento de la organización y podrían generar pérdidas significativas para las mismas. Por lo anteriormente expuesto, las entidades deben tener clasificados los activos de información críticos, con el fin de identificar a tiempo las amenazas y vulnerabilidades que sobre ellos hay, y los riesgos digitales con sus respectivos controles, para poder dar respuestas a las partes interesadas externas e internas en un momento determinado. Por lo anterior, la Corporación Autónoma Regional para el Desarrollo Sostenible del Chocó – CODECHOCÓ, construye este documento denominado plan de tratamiento de riesgos de Seguridad y Privacidad de la información, a través del cual se busca establecer los mecanismos para mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad, Integridad y Disponibilidad de los activos), evitando aquellas situaciones que impidan el logro de los objetivos de la entidad.

Se busca a través de este plan, entre otras cosas, desarrollar una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planeen acciones que reduzcan la afectación a la entidad en caso de materialización. Adicionalmente 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 trazados en el Entorno TIC para la Transformación Digital Sectorial y Territorial e Inclusión Social Digital. Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, Decreto 612 de 2018, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

2. OBJETIVOS

2.1 General

Definir los lineamientos para el tratamiento de los riegos de seguridad y privacidad de la información identificados sobre los activos de información, con el fin de prevenir la materialización de estos y reducir el impacto negativo en la gestión institucional, de aquellos que se lleguen a materializar.

2.2 Específicos

- Definir las actividades requeridas para implementar el tratamiento de riesgos de seguridad de la información.
- Reducir la probabilidad de materialización de un incidente de seguridad de la Información, en la infraestructura tecnológica de la entidad.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos de seguridad de la información.
- Identificar los activos de información que deban protegerse en la entidad.

3. ALCANCE

Este plan será de estricta aplicabilidad y cumplimiento por parte de todos los funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Entidad, y aplica para todos los procesos y actividades desarrolladas por la Entidad, en especial aquellos que impactan directamente la consecución de los objetivos misionales.

4. TÉRMINOS Y DEFINICIONES

- **Activo**: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Aceptación de riesgo**: Decisión de asumir un riesgo
- **Amenazas**: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Análisis de Riesgo**: Uso sistemático de la información para identificar fuentes y estimar el riesgo (Guía ISO/IEC 73:2002). Apetito al riesgo: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.
- **Causa**: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Confidencialidad**: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia**: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Control**: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad.
- **Dueño del riesgo sobre el activo**: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- **Evaluación del riesgo**: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
- **Factor de riesgo**: Agente ya sea humano o tecnológico que genera el riesgo
- **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**: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad**: propiedad de exactitud y completitud.
- **Mapa de riesgos**: documento con la información resultante de la gestión del riesgo.

- **Nivel de riesgo**: Da el resultado en donde se ubica el riesgo por cada activo de información.
- **Probabilidad**: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Riesgo**: Efecto de la incertidumbre sobre el cumplimiento de los objetivos.
- **Riesgo de seguridad digital**: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Riesgo Inherente**: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
- **Riesgo residual**: Nivel restante de riesgo después del tratamiento del riesgo.
- **Tratamiento del riesgo**: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.
- **Tolerancia al riesgo**: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes.
- **Valoración del riesgo**: Proceso de análisis y evaluación del riesgo.
- **Vulnerabilidad**: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

5. ROLES Y RESPONSABILIDADES

A efectos de que quede claro el papel que debe desempeñar cada una de las partes interesadas en la identificación y gestión de riesgos de seguridad de la información, se presenta a continuación la matriz de roles y responsabilidades:

ROLES	RESPONSABILIDADES
Director y Equipo Directivo	• Aprobar la Política de seguridad de la información y sus actualizaciones. • Analizar los cambios en el contexto interno y externo que puedan tener un impacto en la operación de la entidad y generar cambios en la estructura de riesgos y controles.

ROLES	RESPONSABILIDADES
	• Evaluar el estado del Sistema de Control Interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este
Líder de TI	• Diseña el plan de tratamiento de riesgos de seguridad y privacidad de la información de acuerdo con los modelos establecidos por el Gobierno Nacional • Coordinar la formulación y actualización de la política general de seguridad y privacidad de la información, planes y manuales correspondientes para preservar la seguridad digital de la entidad. • Identificar y valorar los riesgos, en conjunto con los líderes de proceso. • Hacer seguimiento al plan de tratamiento de riesgos de seguridad de la información.
Líderes de Proceso	• Identificar y valorar los riesgos de seguridad de la información, asociados a cada proceso. • Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos. • Ejecutar las acciones necesarias con su respectivo seguimiento, para evitar la materialización de los riesgos. • Informar a la Oficina TIC acerca de los riesgos materializados. • Reportar los avances y evidencias de la gestión de los riesgos • Ejecutar las acciones asociadas a los controles establecidos para cada uno de los riesgos. • Mantener la trazabilidad o documentación respectiva de todas las actividades realizadas, para garantizar de forma razonable que dichos riesgos no se materialicen y por ende que los objetivos del proceso se cumplan.
Oficina de Control Interno	• Realizar el seguimiento a los riesgos que a nivel institucional han sido consolidados
Oficina de Prensa y Comunicaciones	• Liderar el proceso de comunicación y consulta del plan

Tabla 1: Matriz de Roles y responsabilidades

6. METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En la figura siguiente se presenta el modelo de gestión de riesgos de seguridad de la información basado tanto en la norma ISO/IEC 31000 como en la ISO 27005 para la adecuada

administración de riesgos en la seguridad de la información; los elementos que lo componen son:

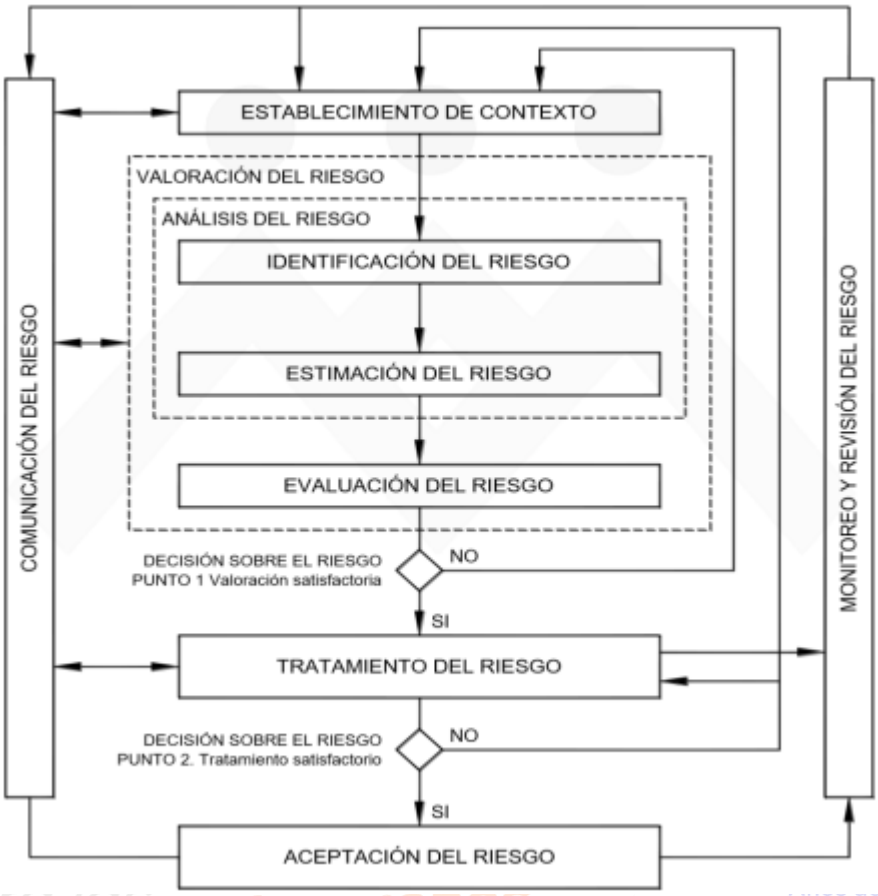

Ilustración 1: Metodología para la administración del riesgo – Fuente: Guía para la administración del riesgo – DAFP

6.1. Establecimiento del contexto

- **<u>Contexto Interno</u>**: El contexto interno considera factores que impactan directamente a:
  - CODECHOCÓ en general como organización, sistemas de información o servicios, reglamentación interna, número de sedes, empleados, entre otros aspectos.
  - Cada uno de los procesos sobre los cuales están soportadas las operaciones de la entidad.

- **<u>Contexto Externo</u>**: para determinar este contexto, CODECHOCO debe considerar los siguientes factores relacionados con el contexto digital:
  - Clientes y proveedores de servicios que se relacionen con la misión de la entidad pública analizada.
  - Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad; ejemplo, la ley 1581 de 2012 o la ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el decreto 1078 de 2015 o el decreto 1499 de 2017.
  - Entorno cultural.
  - Cantidad de ciudadanos a los cuales la entidad pública brinda servicios a través del entorno digital como trámites a través de páginas web. Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, tales como el ambiente social, eco económico y ambiental que tengan alguna relación con las operaciones asociadas a la secretaria distrital de gobierno.

- **<u>Identificación de Activos de información</u>**

  Según la norma ISO 27000 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. Por consiguiente, dentro del proceso de gestión tecnológica, la entidad elaboró y publicó el inventario y clasificación de activos de información, el cual se actualiza de acuerdo con las necesidades, a la fecha se encuentra en su versión 2.0 y tiene definidos los activos de tipo información o datos, servicio, aplicación, equipo informático, dispositivo, etc., los cuales se encuentran debidamente clasificados de acuerdo la NTC 270001, al Decreto 103 de 2015 y a la Ley 1581 de 2012.

6.2. Identificación de riesgos

La identificación de los riesgos inherentes de seguridad digital se lleva a cabo analizando las amenazas internas y externas a las que están expuestos los activos de la información de la entidad; las cuales se cruzan con las vulnerabilidades en el entorno digital, resultando así la definición de los riesgos existentes y que puede afectar el logro de objetivos y vulnerar algunos de los pilares de la seguridad de la información (integridad, disponibilidad,

confidencialidad). Este análisis incluye aspectos relacionados con el ambiente físico, digital y las personas.

El propósito de la identificación del riesgo digital es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida.

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas)

Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

A continuación, se describen una serie de amenazas comunes:

D= Deliberadas, A= Accidentales, E= Ambientales

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	E
	Perdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	
Perturbación debida a la radiación	Radiación electromagnética	
	Radiación térmica	
	Impulsos electromagnéticos	
Compromiso de la información	Interceptación de señales de interferencia comprometida	
	Espionaje remoto	
	Escucha encubierta	
	Hurto de medios o documentos	
	Hurto de equipo	
	Recuperación de medios reciclados o desechados	

TIPO	AMENAZA	ORIGEN
	Divulgación	
	Datos provenientes de fuentes no confiables	
	Manipulación con hardware	
	Manipulación con software	
	Detección de la posición	
Fallas técnicas	Fallas del equipo	
	Mal funcionamiento del equipo	
	Saturación del sistema de información	
	Mal funcionamiento del software	
	Incumplimiento en el mantenimiento del sistema de información.	
Compromiso de las funciones	Error en el uso	
	Abuso de derechos	
	Falsificación de derechos	
	Negación de acciones	
	Incumplimiento en la disponibilidad del personal	

Tabla 2: Amenazas comunes Fuente: ISO/EIC 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.

A continuación, se relacionan algunas vulnerabilidades conocidas y que pueden ser tenidas en cuenta:

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento
	Ausencia de esquemas de reemplazo periódico
	Susceptibilidad a la humedad, el polvo y la suciedad
	Sensibilidad a la radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
	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" cuando se abandona la estación de trabajo
	Ausencias de pistas de auditoria
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario

	Tablas de contraseñas sin protección
	Software nuevo o inmaduro
RED	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables
	Punto único de fallas
PERSONAL	Ausencia del personal
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
	Falta de conciencia acerca de la seguridad
	Ausencia de mecanismos de monitoreo
	Trabajo no supervisado del personal externo o de limpieza
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
	Ubicación en área susceptible de inundación
	Red energética inestable
	Ausencia de protección física de la edificación (Puertas y ventanas)
ORGANIZACIÓN	Ausencia de procedimiento y/o políticas en general
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad

Tabla 3: Vulnerabilidades comunes Fuente: ISO/EIC 27005:2009

A continuación, se presentan ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas:

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Tabla 4: Tabla de Amenazas vs Vulnerabilidades Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

6.3. Valoración/Estimación del riesgo

La valoración o estimación del riesgo inherente, consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

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 recuperación.	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 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.
CATASTRÓFICO	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.	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.

Tabla 5: Criterios para calificar el impacto – Riesgos de Seguridad Digital. Fuente: DAFP

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.

Tabla 6: Criterio para calificar la probabilidad de ocurrencia. Fuente: DAFP

6.4. Evaluación de riesgos

En esta etapa Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

Haciendo uso de la matriz denominada "Matriz de Calificación, Evaluación y respuesta a los Riesgos se definen los niveles de impacto y probabilidad, así como las zonas de riesgo presentando las posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen:

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Tabla 7: "Matriz de Calificación, Evaluación y respuesta a los Riesgos" Fuente: Guía de Riesgos DAFP

6.5. Tratamiento de riesgos

De acuerdo con la valoración de los riesgos de seguridad digital realizada, se procede a tomar acciones (definir los controles), que serán aplicados por los responsables de los riesgos (líderes de procesos) y permitirán darles el tratamiento correspondiente, que puede ser: reducirlos, evitarlos, transferirlos o compartirlo, aceptarlo:

- Reducir el riesgo: tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención) como el impacto (medidas correctivas).
- Evitar el riesgo: tomar las medidas encaminadas a prevenir su materialización, decidir no iniciar o continuar la actividad que lo originó.
- Compartir o transferir el riesgo: reduce su efecto compartiéndolo con una o varios de los procesos o partes (incluyendo los contratos y la financiación del riesgo).
- Aceptar el riesgo: decisión que toma el dueño del riesgo de aceptar las consecuencias y probabilidad de un riesgo en particular. Retener el riesgo mediante una decisión informada. Esta opción solo puede aplicarse para los riesgos que se encuentren en el nivel bajo.

Las acciones para emprender pueden ser de tipo preventivas (actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización) o correctivas (permiten el establecimiento de la actividad, después de ser detectado un evento no deseado), y están representadas en políticas, procedimientos, guías, lineamientos o demás, que permitan controlar y hacer seguimiento sobre la gestión realizada a los riesgos.

En razón a esto, la formulación de políticas deberá contemplan los objetivos a alcanzar, una estrategia de cómo se desarrollarán las políticas a corto, mediano y largo plazo, indicar qué riesgos se van a priorizar y controlar, estimar los recursos necesarios y finalmente hacer seguimiento a la efectividad de las políticas de administración de riesgos de seguridad digital definidas.

Con base en el resultado del análisis de riesgo se debe definir el tratamiento que deba dársele a cada uno, así:

TRATAMIENTO DE RIESGOS		
TIPO DE RIESGO	**ACCIÓN REQUERIDA**	**TRATAMIENTO**
Catastrófico	Requiere acciones inmediatas para evitar la pérdida de la confidencialidad, integridad y disponibilidad de la información	Reducir, evitar o compartir
Alto	Requiere de acciones rápidas por parte de la Alta Dirección para disminuir el riesgo.	Reducir, evitar o compartir
Moderado	Se requiere seguir ejecutando los controles definidos para el riesgo y revisar eficacia de estos.	Reducir, evitar o compartir
Bajo	El riesgo se mitiga con actividades propias y por medio de acciones detectivas y preventivas.	Aceptar
Insignificante	El riesgo no representa impacto significativo para la Entidad	Aceptar

Tabla 8: Tratamiento de riesgos

6.6. Monitoreo y revisión

Dado que el origen y tipos de riesgos son variables, el monitoreo constante será necesario para detectar cambios respecto a nuevos activos de información, nuevos procesos o procedimientos, nuevos factores o amenazas que afecten los activos de información, nuevas vulnerabilidades, incremento el impacto e incluso la materialización de incidentes de seguridad digital.

Para llevar a cabo este monitoreo se definen las siguientes acciones:

- Registro y reportes de incidentes de seguridad digital
- Reporte de la gestión de riesgos de seguridad digital al interior de la entidad.
- Reportes de la gestión de riesgos de la seguridad digital a autoridades o entidades especiales.
- Auditorías internas y externas
- Medición de desempeño.

6.7. Seguimiento

La entidad trabajará en la mejora continua de la gestión de riesgos de seguridad digital, velando por la mitigación de vulnerabilidades, amenazas, riesgos, eventos e incidentes que

atenten contra la disponibilidad, integridad y confidencialidad de la información asociada a los distintos activos de información, como parte de los procesos de la entidad; y se llevaran a cabo las acciones necesarias para atender los hallazgos o no conformidades producto de auditorías internas y externas.

El seguimiento y la revisión son una parte importante del proceso de Gestión de Riesgos, donde las responsabilidades de seguimiento, monitoreo y evaluación deben estar claramente definidas y deben abarcar todos los aspectos del proceso de gestión. El responsable del seguimiento del presente plan es el Líder de TI, en coordinación con los líderes de procesos.

Dentro de las actividades que se ejecutan en esta fase, se tienen:

- Analizar los cambios, las tendencias, los éxitos y los fracasos dentro del proceso de gestión de riesgos de seguridad de la información.
- Detectar cambios en el contexto interno o externo, incluyendo los cambios que se puedan presentar en los criterios de riesgos de seguridad de la información.
- Revisar la implementación de los planes de tratamiento de riesgo de seguridad de la información y las prioridades de implementación de estos.
- Identificación de nuevos riesgos de seguridad de la información.

La revisión de la gestión de riesgos se debe hacer por lo menos una vez al año, el seguimiento a los riesgos debe ser permanente por parte de los líderes de los procesos.

El seguimiento a este plan permite direccionar el riesgo a una mejora continua, adoptando nuevos procedimientos o mecanismos para ser más predictivos con las nuevas amenazas, que se puedan identificar tempranamente desde el ciberespacio.

6.8. Comunicación y consulta

La comunicación y consulta debe estar presente durante todas las etapas del proceso para la gestión del riesgo, ya que esto permite garantizar que se tengan en cuenta las necesidades e intereses de todas las partes interesadas en los procesos y por consiguiente involucrados de alguna manera en la identificación y gestión de los riesgos identificados. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

Con el apoyo de la oficina de comunicaciones se genera una estrategia de comunicaciones que permita dar a conocer este plan de tratamiento y todo lo que incluye.

La comunicación y consulta permite:

- Establecer correctamente el contexto para los procesos
- Garantizar que se tomen en consideración las necesidades de los usuarios
- Garantizar que los riegos estén correctamente identificados
- Reunir diferentes áreas de experticia para el análisis de los riesgos
- Garantizar que los diferentes puntos de vista se toman en consideración adecuadamente durante todo el proceso
- Fomentar la administración del riesgo como una actividad inherente al proceso de planeación estratégica

7. RECURSOS

CODECHOCÓ, en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), requiere de los siguientes recursos:

RECURSOS	DESCRIPCIÓN
Humanos	- Profesional especialista en seguridad digital - Grupo interno de seguridad y privacidad de la información - Líderes de procesos
Tecnológicos	- Firewall – licencia - Antivirus - Servicios: internet, almacenamiento en nube - Unidades de almacenamiento
Técnico	- Herramientas para la gestión del riesgo: guía, planes, matriz de riesgos
Financieros	- Recursos para la adquisición de conocimientos - Recursos para la contratación de personal - Recursos para la Contratación de auditorías externas - Recursos para capacitaciones institucionales sobre seguridad de la información

Tabla 9: Recursos

8. PLAN DE IMPLEMENTACIÓN

No	ACTIVIDAD	TAREA	RESPONSABLE	PRODUCTO/ENTREGABLE	FECHA	
					INICIAL	FINAL
1	Actualización de lineamientos para la gestión de riesgos	Documentar y aprobar los procedimientos y/o documentos relacionados con seguridad de la Información	Oficina TIC	Documentos y actas de aprobación	1-feb	31-mar
2	Sensibilización	Socializar los lineamientos y herramientas para la Gestión de los Riesgos de Seguridad y privacidad de la Información.	Oficina TIC	Listados de asistencia, registro fotográfico, memorias (grabación)	1-mar	30-may
3	Identificación de Riesgos de Seguridad y Privacidad de la Información	Establecer el contexto institucional en relación con la seguridad de la información. (Debilidades, oportunidades, fortalezas y amenazas)	Líderes de procesos y sus equipos de trabajo	Documento plan de tratamiento de riesgos	1-mar	30-may
4		Identificar o actualizar los activos de información de los procesos institucionales	Líderes de procesos y sus equipos de trabajo	Matriz de activos de información actualizada	1-feb	30-abr
5		Identificar, analizar y evaluar los riesgos de seguridad y privacidad de la información	Oficina TIC en conjunto con los líderes de procesos	Matriz de riesgos de seguridad y privacidad de la información	1-mar	30-may
6		Revisar, verificar y retroalimentar los riesgos identificados.	Oficina TIC	Matriz de riesgos de seguridad y privacidad de la información	1-mar	30-may
7	Aceptación de Riesgos Identificados	Aprobar los riesgos identificados y elaborar los planes de tratamiento cuando aplique	Oficina TIC en conjunto con los líderes de procesos	Correos electrónicos, controles establecidos sobre cada riesgo	1-jun	31-jul
8	Seguimiento	Realizar el seguimiento a la implementación de controles y planes de tratamiento para los riesgos identificados	Todos	Matriz de seguimiento	31-jul	31-dic
9	Mejoramiento	Identificar oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento de los riesgos de seguridad y privacidad de la información.	Todos los procesos	Actas de reunión para identificar oportunidades de mejora	31-jul	31-dic
10		Revisar o actualizar los lineamientos de Riesgos de Seguridad y privacidad de la información	Oficina TIC	Documentos actualizados	31-jul	31-dic
11		Ajustar los mapas de riesgos de seguridad y privacidad de la información en lo relacionado con controles, vulnerabilidades o responsables.	Oficina TIC en conjunto con los líderes de procesos	Matriz de riesgos de seguridad y privacidad de la información actualizada	31-jul	31-dic

Adicionalmente, utilizando el modelo de matriz para definición de riesgos, diseñada para el DAFP para tal fin, se realizó la identificación, valoración y tratamiento de los riesgos digitales para cada proceso. Ver Matriz de riesgos de seguridad de la información.

Proyecto/Elaboró	*Aprobó*	*Folios*	*Anexos*	*Folios de anexos*	*Fecha*
Jenixe Mena *Profesional Especializado*	*Jenixe Mena* *Profesional Especializado*	*21*			*Enero - 2024*