Agencia Nacional de Infraestructura

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

G.I.T DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES

ELABORÓ:	REVISÓ:	APROBÓ:
Guillermo Cadena Ronderos **Asesor G.I.T de Tecnologías de la Información y las Telecomunicaciones**	Andres Francisco Boada **Coordinador G.I.T de Tecnologías de la Información y las Telecomunicaciones**	Diego Alejandro Morales Silva **Vicepresidente de Planeación, Riesgos y Entorno.** Andrés Francisco Boada **Coordinador G.I.T de Tecnologías de la Información y las Telecomunicaciones**
FECHA: 31/01/2020	**FECHA:** 31/01/2020	**FECHA:** 31/01/2020

Tabla de contenido

1. OBJETIVOS GENERAL 3
2. CONTEXTO 3
3. ALCANCE 4
4. LINEAMIENTOS DE EJECUCIÓN 4
5. DOCUMENTOS RELACIONADOS 4
6. METODOLOGÍA DE EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 4
6.1 IDENTIFICACIÓN DE RIESGOS 5
6.2 VALORACIÓN DE LOS RIESGOS 6
6.2.1 Identificación de amenazas 7
6.2.2 Identificación de las Vulnerabilidades. 8
6.3 ANÁLISIS DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN 9
6.4 EVALUACIÓN DE LOS CONTROLES ESTABLECIDOS PARA LA MITIGACIÓN DE LOS RIESGOS 12
6.5 TRATAMIENTO 14
6.6 SEGUIMIENTO Y REVISIÓN DEL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 15
7. terminos y definiciones. 15

1. OBJETIVOS GENERAL

Definir los lineamientos y metodología a seguir para el análisis, valoración y tratamiento de riesgos de Seguridad, alineados con las políticas de seguridad y privacidad de la información

OBJETIVOS ESPECIFICOS

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Definir los principales activos a proteger en la Agencia.
- Identificar las principales amenazas que afectan a los activos.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información

2. CONTEXTO.

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Es muy importante que las organizaciones cuenten con un plan de gestión de riesgos para garantizar la continuidad del negocio. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en La Agencia Nacional de Infraestructura. Previo a este ejercicio, es importante conocer la situación actual de la agencia y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las entidades. Una organización sin un plan de gestión de riesgos está expuesta a perder su información.

El plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal de la ANI a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

Son requisitos indispensables para la implementación del presente plan:

- Lograr el compromiso de la alta gerencia de la ANI para emprender la implementación del plan de gestión del riesgo en la seguridad de la información.
- Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.
- Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

3. ALCANCE

La identificación y tratamiento de los riesgos de seguridad de la información como lineamiento de la alta gerencia de la ANI, 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; dicho tratamiento de riesgo debe involucrar a todos los procesos y actividades desarrolladas por la Entidad, en especial aquellos que impactan directamente la consecución de los objetivos misionales.

4. LINEAMIENTOS DE EJECUCIÓN

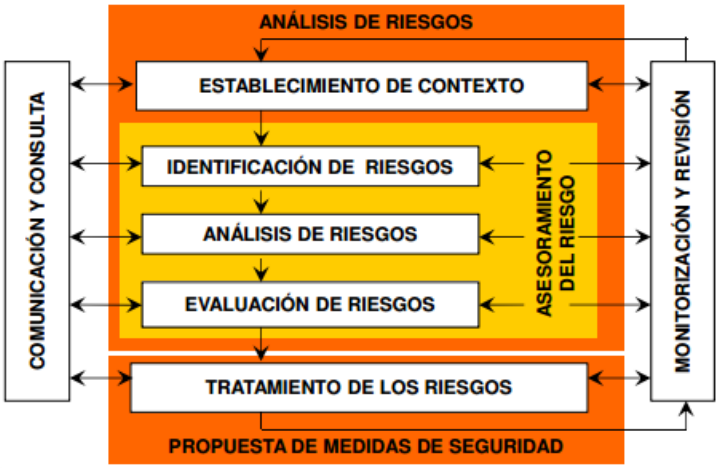
- Los líderes de procesos con el apoyo del G.I.T de Tecnologías de la Información las Telecomunicaciones, son responsables de la aplicación adecuada y oportuna de la presente guía
- En el proceso de valoración de riesgos deben estar involucrados todos los líderes de proceso, dueños de la información y por ende dueños del riesgo.
- El plan de tratamiento de riesgos definido en este documento debe estar aprobado por los líderes de procesos.
- Se ejecutará un análisis de riesgos anual o cuando necesario realizar actualizaciones por cambios significativos en la operación de la Agencia, en cabeza de los líderes de los procesos y el Grupo de Planeación de la ANI

5. DOCUMENTOS RELACIONADOS

- Política General de Seguridad y Privacidad de la Información (GTEC-P-XXX)
- Manual de Políticas Específicas de Seguridad y Privacidad de la Información (GTEC-P-XXX)
- Norma ISO 31000:2009
- Inventario de activos de información

6. METODOLOGÍA DE EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La Agencia Nacional de Infraestructura – ANI, utiliza una metodología de Gestión de Riesgos de Seguridad de la Información alineada con la norma ISO 31000:2009. Las actividades que hacen parte de la metodología son las siguientes:



ETAPAS DE LA GESTIÓN DE RIESGOS

La ANI, ha definido que su gestión de riesgos consiste en la identificación, evaluación, análisis, monitoreo y comunicación de riesgos críticos para cada uno de los procesos y/o áreas de mayor criticidad dentro de la organización, es decir, aquellas que se encuentren directamente ligadas con la protección y creación de valor de la Agencia.

Igualmente se ha determinado que el presente plan se dará por cumplido cuando se realicen todas las fases del ciclo de la metodología y el tiempo se determinará una vez iniciado cada ciclo.

A continuación, se detallan las distintas etapas de la metodología de gestión de riesgos:

6.1 IDENTIFICACIÓN DE RIESGOS

El objetivo de esta etapa es identificar los principales riesgos críticos a los cuales se encuentran expuestos los procesos de la Agencia. Los encargados de Riesgos identificarán, para los procesos de su responsabilidad, los riesgos críticos que pudieran afectar los objetivos y/o estrategias definidas para el área. Dicha identificación puede ser realizada a través de los siguientes métodos:

- Reuniones o workshop con el equipo de trabajo.
- Encuestas a los distintos participantes del equipo de trabajo.
- Bases de datos o matices de riesgo de ejercicios previos.

Una vez Identificados los riesgos críticos, estos se deben documentar en una matriz de riesgos, clasificándolos por tipo de riesgo de acuerdo con lo siguiente:

- Estratégico: Riesgo relacionado con los objetivos estratégicos, alineados con la misión de la Agencia.

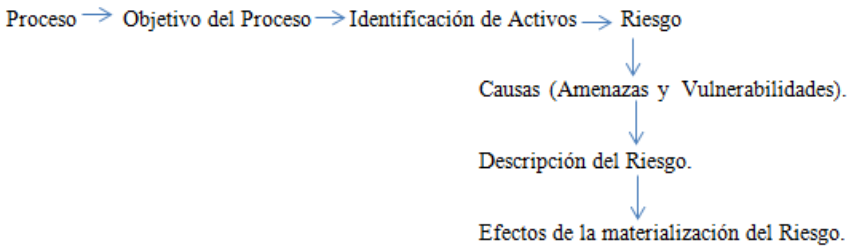
- De Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la Agencia.
- Financieros: Riesgo relacionado con el uso eficaz y eficiente de los recursos financieros.
- Operacional: Riesgo resultante de deficiencias o fallas en procesos, personas, sistemas o eventos externos.
- Tecnológicos: Están relacionados con la capacidad tecnológica de la ANI para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
- Cumplimiento: Riesgo relacionado con el cumplimiento de leyes y regulaciones, especialmente concierne al cumplimiento de aquellas leyes y normas a las cuales la ANI está sujeta.

6.2 VALORACIÓN DE LOS RIESGOS

El objetivo de este paso es generar una lista completa de los riesgos sobre la base de los acontecimientos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos de la Agencia.

Las debilidades de los procesos en cuanto a seguridad de la información, los riesgos a los cuales se encuentran expuestos y las causas que podrían comprometer la confidencialidad, integridad y disponibilidad de los procesos de la ANI deben ser identificadas y evaluadas teniendo en cuenta los criterios de evaluación definidos. En este proceso se debe realizar las siguientes actividades:

- Identificar el flujo de información de cada uno de los procesos
- Identificar las vulnerabilidades que existen en el proceso.
- Identificar las amenazas que podrían materializarse, dadas las vulnerabilidades existentes.
- Definir las escalas a utilizar



De acuerdo con los Lineamientos para la gestión de riesgos digital en entidades públicas emitida por el DAFP, 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:

6.2.1 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).

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	F
	Fenómenos sísmicos	F
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	F,D,A
Pérdidas de los servicios esenciales	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

Tipo	Amenaza	Origen
	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
Dirigidas por el hombre	Piratería	D
	Ingeniería social	D
	Crimen por computador	D
	Acto fraudulento	D
	Ataques contra el sistema	D
	DDoS	D
	Penetración en el sistema	D
	Ventaja de defensa	D
	Hurto de información	D
	Asalto a un empleado	D
	Chantaje	D

6.2.2 Identificación de las Vulnerabilidades.

Se deben identificar vulnerabilidades (debilidades) de acuerdo con los siguientes tipos:

Tipo	Vulnerabilidad
Hardware	Mantenimiento insuficiente
	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

Tipo	Vulnerabilidad
	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)

6.3 ANÁLISIS DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

El objetivo del Análisis de Riesgos es identificar y valorar los riesgos a los cuales están expuestos los procesos y los flujos de información, para identificar y seleccionar los controles apropiados de seguridad. El análisis está basado en los flujos de información de cada uno de los procesos y los requerimientos de seguridad, tomando en cuenta los controles existentes.

En esta etapa se definen los criterios que se deben utilizar para evaluar la importancia del riesgo. Los criterios reflejarán los valores de la Agencia, los objetivos y los recursos existentes. Estos criterios de riesgo estarán revisándose de forma permanente, dado los cambios que pueden ocurrir en la organización.

Al definir los criterios de riesgo, se tendrán en cuenta:

- La naturaleza, los tipos de causas y consecuencias que pueden ocurrir y como se van a medir.
- La manera de definir la probabilidad de ocurrencia de un evento.
- La forma de determinar el nivel de riesgo.
- Niveles de riesgo aceptable para la organización.

Las actividades realizadas para ejecutar el análisis de riesgos se realizan de acuerdo con el siguiente esquema:

- Definición de las áreas de la ANI que se incluirán dentro del alcance del proceso de gestión de riesgos de seguridad digital y ciberseguridad.
- Levantamiento de información relacionada con el proceso seleccionado.
- Entrevistas con personas claves dentro del proceso para conocer su percepción del riesgo al cual se encuentra expuesta la información.
- Ejecución de la evaluación de riesgos a los que se encuentra expuesto el proceso, por medio de valoración de hallazgos y evaluación de probabilidad de ocurrencia de amenazas y vulnerabilidades.
- Análisis y diagnóstico del nivel de riesgo para el proceso definido. Se llevará a cabo la elaboración de informe de resultados.

Para la identificación de Amenazas, vulnerabilidades y riesgos, se tienen en cuenta los resultados de las entrevistas con los dueños y/o responsables de los procesos del negocio y los análisis de riesgos existentes. Con el fin de establecer los niveles de riesgos a los cuales se encuentran expuestos los procesos, se mide la probabilidad de ocurrencia de las amenazas y el impacto que tendría las consecuencias de su materialización.

Se determina la probabilidad de ocurrencia para cada riesgo de acuerdo con la siguiente escala:

Valoración asignada	Valor Asignado	Frecuencia
Insignificante	1	Ha ocurrido una vez en los últimos tres a cinco años
Bajo	2	Ha ocurrido una vez en los últimos >= tres y < cinco años
Moderado	3	Ha ocurrido >= una vez en el período >= un año y < tres años
Mayor	4	Ha ocurrido entre una y tres veces en el último año
Catastrófico	5	Ha ocurrido más de tres veces en el último año

Se determina el impacto de cada riesgo de acuerdo con la siguiente escala:

Valoración asignada	Valor Asignado	IMPACTO CUANTITATIVO	IMPACTO CUALITATIVO
Insignificante	1	Afectación <= 1% de la población.	Sin afectación de la integridad.
		No hay afectación medioambiental	Sin afectación de la disponibilidad.
		No hay afectación a la divulgación / no hay fuga de información	Sin afectación de la confidencialidad.
Bajo	2	Afectación <= 2% de la población.	Afectación leve de la integridad.
		Afectación <=1% del presupuesto anual de la entidad.	Afectación leve de la disponibilidad.
		Afectación leve del medio ambiente requiere de 1 semanas de recuperación.	Afectación leve de la confidencialidad.
Moderado	3	Afectación <=5% de la población.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros.
		Afectación <=3% del presupuesto anual de la entidad.	Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros.

Valoración asignada	Valor Asignado	IMPACTO CUANTITATIVO	IMPACTO CUALITATIVO
		Afectación leve del medio ambiente requiere de 3 semanas de recuperación.	Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
Mayor	4	Afectación <=10% de la población.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros.
		Afectación <=5% del presupuesto anual de la entidad.	Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.
		Afectación importante del medio ambiente que requiere de <=2 meses de recuperación.	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
Catastrófico	5	Afectación <=30% de la población.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros.
		Afectación <=10% del presupuesto anual de la entidad.	Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.
		Afectación muy grave del medio ambiente que requiere de <=2 años de recuperación.	Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

6.4 EVALUACIÓN DE LOS CONTROLES ESTABLECIDOS PARA LA MITIGACIÓN DE LOS RIESGOS

La Evaluación de los controles se realiza cuando se ha establecido el riesgo inherente para los procesos y el impacto y probabilidad de ocurrencia de cada uno de los riesgos establecidos. La evaluación de controles se realiza identificando los criterios relacionados a cada uno de los riesgos establecidos.

VARIABLES:

CARACTERISTICA	DESCRIPCION
Naturaleza del Control	Determina si el control es manual, mixto o automático
Documentación	Establece si el control está documentado (si) / no está documentado (no)
Evidencia	Si el control está Divulgado o no divulgado
Tipo de control	Control: detectivo, preventivo o correctivo

Para cada tipo de control se tienen los siguientes pesos para determinar su eficacia:

TIPO DE CONTROL	PESO
Manual, mixto o automático	25%
Documentado (si) / no está documentado (no)	25%
Detectivo, preventivo o correctivo	25%
Divulgado o no divulgado	25%

COBERTURA EFECTIVA: Con este análisis se identifica que en porcentaje se está mitigando el control teniendo en cuenta los siguientes determinadores:

NIVEL DE COBERTURA	PESO
Más del 90%	10
Entre 80 y 90%	9
Entre 70 y 80%	8
Entre 60 y 70%	7
Entre 50 y 60%	6
Entre 40 y 50%	5
Entre 30 y 40%	4

NIVEL DE COBERTURA	PESO
Entre 20 y 30%	3
Entre 10 y 20%	2
Menos del 10%	1

6.5 TRATAMIENTO

Con base en el resultado del análisis de riesgo y con el fin de tratar el riesgo residual se debe establecer los niveles de riesgo y adelantar acciones de mejora que propenden por conservar las características de confidencialidad, integridad y disponibilidad de la información.

NIVELES DE RIESGOS			
Tipo de riesgo	**Valor Asignado**	**Acción requerida**	**Gestión requerida**
Riesgo Catastrófico	Mayor a 12	Requiere acciones inmediatas para evitar la pérdida de la confidencialidad, integridad y disponibilidad de la información	Mitigar
Riesgo Alto	>8 y <= 10	Requiere de acciones rápidas por parte de la Alta Dirección para disminuir el riesgo.	Mitigar
Riesgo Moderado	>5 y <= 8	Se requiere seguir ejecutando los controles definidos para el riesgo y revisar eficacia de estos.	Mitigar
Riesgo Bajo	>= 2 y <=4	El riesgo se mitiga con actividades propias y por medio de acciones detectivas y preventivas.	Aceptar
Riesgo insignificante	1	El riesgo no representa impacto significativo para la Entidad	Aceptar

Las opciones de tratamiento de riesgos según ISO 31000:2018 no son excluyentes entre sí. Tampoco resultan eficaces en todas las circunstancias. Éstas pueden incluir una o varias de las siguientes acciones:

- Eliminar el riesgo prescindiendo del proceso, la actividad o las circunstancias que lo generan.

- Asumir el riesgo, aun aumentándolo, con el fin de incrementar una posible oportunidad.
- Tomar acciones para disminuir la probabilidad del riesgo.
- Implementar acciones que disminuyan el impacto negativo del riesgo.
- Compartir el riesgo (cláusulas en contratos o comprar pólizas de seguros)
- Retener el riesgo con base en información confiable.

Se deben tener en cuenta los siguientes factores en el establecimiento del tratamiento del riesgo.

a) Si se encuentra en una zona de aceptación o apetito de riesgo.
b) Recibirán tratamiento todos los riesgos que tengan un nivel de exposición Alto y Extremo
c) Si es susceptible de ser tratado a través de la implantación de un nuevo control o fortaleciendo los ya existentes.
d) Si la decisión es aceptarlo, independiente de donde se encuentre ubicado y la afectación que pueda tener para Confidencialidad, Integridad y Disponibilidad de la información.
e) Si se decide ignorar el riesgo se reinicia el análisis

6.6 SEGUIMIENTO Y REVISIÓN DEL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

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 Coordinador G.I.T de Tecnología de la Información y la Telecomunicaciones de la ANI en coordinación con el área de planeación de la entidad como área que lidera y articula los procesos en la ANI

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 6.6 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.

7. terminos 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. Para el riesgo de corrupción la tolerancia es inaceptable.

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.