SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

INTRODUCCIÓN

La información que hace parte del Instituto para el Desarrollo de Antioquia - IDEA es crucial para su correcto desempeño y es primordial para el cumplimiento de sus objetivos. Es necesario que el Instituto tenga un enfoque sistemático para la administración del riesgo en la seguridad de la información y ciberseguridad, siendo adecuado para su entorno y en particular, debería cumplir los lineamientos de toda la gestión del riesgo Institucional.

La administración del riesgo en la seguridad de la información y ciberseguridad debe aplicar a todo el Instituto y debe ser una parte integral de todas las actividades de gestión de seguridad de la información y ciberseguridad que se realicen, analizando siempre lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo.

Esta guía está basada en las normas técnicas NTC-ISO 27005, ISO 31000:2018 y en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas de la Función Pública, y formará parte del Modelo de Seguridad de la Información y Ciberseguridad del IDEA.

1. OBJETIVO

Establecer un marco de administración de riesgos de seguridad de la información y ciberseguridad, que permita identificar las amenazas y vulnerabilidad que puedan afectar la confidencialidad, integridad y disponibilidad de la información del Instituto.

2. ALCANCE PARA LA ADMINISTRACIÓN DEL RIESGO

La administración del riesgo de seguridad de la información y ciberseguridad es aplicable a todos los procesos y activos de información del IDEA.

3. NORMATIVIDAD

Ver normograma.

4. DEFINICIONES

- ACTIVO DE INFORMACIÓN: Es toda la información misional, operativa y administrativa que el Instituto recibe o produce y que es considerada de alta validez. Incluye la información impresa,

escrita, trasmitida o almacenada en cualquier medio electrónico, equipo de cómputo, software, hardware y datos contenidos en registros, archivos, bases de datos, videos e imágenes.

- AMENAZAS: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización

- APETITO AL RIESGO: Magnitud y tipo de riesgo que una organización está dispuesta a aceptar

- CAUSA: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

- CIBERAMENAZA: Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

- CIBERATAQUE: Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

- CIBERESPACIO: Entorno complejo resultante de la interacción de personas, software y servicios en internet a través de dispositivos tecnológicos conectados a dichas red, el cual no existe en ninguna forma física.

- CIBERIESGO: Posible resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.

- CIBERSEGURIDAD: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio

- CSIRT (Computer Security Incident Response Team) : Equipo responsable del desarrollo de medidas preventivas y de respuesta a incidentes informáticos.

- CONSECUENCIA: Los efectos o situaciones resultantes de la materialización del riesgo que impacta en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- CONTEXTO EXTERNO: Ambiente externo en el cual la organización busca alcanzar sus objetivos.

- CONTEXTO INTERNO: Ambiente interno en el cual la organización buscar alcanzar sus objetivos

- CONTROL: Medida que modifica al riesgo. Medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

- ESTABLECIMIENTO DEL CONTEXTO: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo.

- EVALUACIÓN DEL CONTROL: Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces

- EVALUACIÓN DEL RIESGO: 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.

- EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles.

- FRECUENCIA: Medición del número de ocurrencias por unidad de tiempo.

- GESTIÓN DEL RIESGO: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo

- GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

- IDENTIFICACIÓN DEL RIESGO: Proceso para encontrar, reconocer y describir el riesgo

- INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones.

- IMPACTO: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

- MAPA DE RIESGOS: Documento con la información resultante de la gestión del riesgo

- NIVEL DE RIESGO: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad

- PROBABILIDAD: Posibilidad de ocurrencia del riesgo, puede ser medida con criterios de frecuencia o factibilidad.

- REDUCCIÓN DEL RIESGO: Acciones que se toman para disminuir la probabilidad, las consecuencias negativas o ambas, asociadas a un riesgo.

- RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN: una amenaza determinada explote la vulnerabilidad de un activo pudiendo causar un daño.

- RIESGO INHERENTE: Es aquel riesgo al que se enfrenta la entidad en ausencia de controles o acciones que mitiguen la probabilidad o el impacto.

- RIESGO RESIDUAL: Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.

- TRATAMIENTO DEL RIESGO: Proceso para modificar el riesgo

- TOLERANCIA AL RIESGO: Son los niveles aceptables de desviación relativa a la consecución de objetivos.

- SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas.

- VALORACIÓN DEL RIESGO: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo

- VULNERABILIDAD: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas

5. ORGANIZACIÓN PARA LA GESTIÓN DEL RIESGO

5.1 Definición de Roles y Responsabilidades

Se describen todos los roles y responsabilidades de la Junta Directiva, Gerente General, Directivos, Oficina Gestión del Riesgos, Dirección de Sistemas, Control Interno, Comité de Seguridad de la Información y Ciberseguridad, Servidores Públicos y Contratistas.

6. IDENTIFICACIÓN DE RIESGOS

En esta etapa se deben establecer las fuentes o factores de riesgo, las vulnerabilidades, las amenazas, los eventos o riesgos, y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas (NTC ISO31000, Numeral 2.15).

6.1 Establecimiento del Contexto

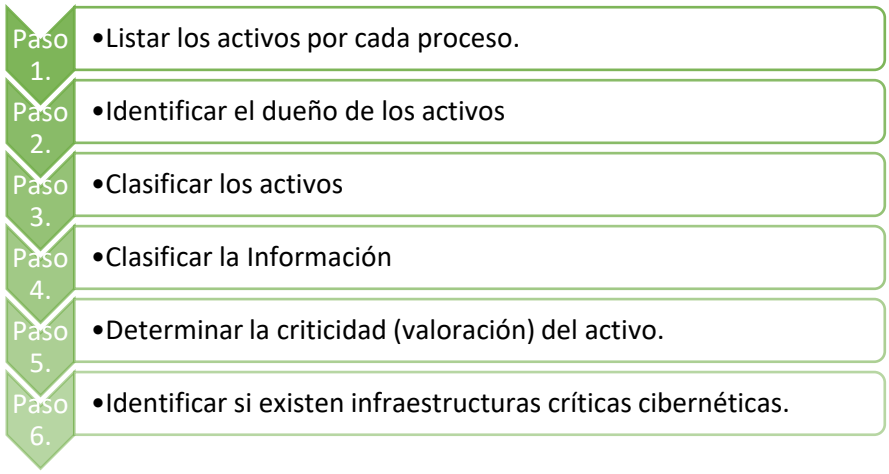
Es la definición de los parámetros internos y externos que tomaran en consideración para la administración del riesgo, esto ayuda en la identificación de las causas de los riesgos.

En la medida en que se vayan presentando cambios en el contexto, se pueden presentar nuevos eventos o riesgos que deben ser atendidos como parte del proceso.

Se puede tener en cuenta el análisis situacional y las herramientas utilizadas para establecer el PEI, enfocándose en la seguridad de los activos de información.

6.2 Identificación, Clasificación y Valoración de Activos

El proceso de identificación, clasificación y valoración de activos de información se realiza de acuerdo a la "Guía para la Gestión de Activos de Información" la cual forma parte del Modelo de Seguridad de la Información y Ciberseguridad del IDEA:



6.3 Metodología para el Análisis de Riesgos

El propósito de la identificación del riesgo es determinar que podría suceder que cause una pérdida potencial, las preguntas claves para la identificación del riesgo permiten determinar:

¿QUÉ PUEDE SUCEDER?

Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.

¿CÓMO PUEDE SUCEDER?

Establecer las causas a partir de los factores determinados en el contexto

¿CUÁNDO PUEDE SUCEDER?

Determinar de acuerdo al desarrollo del proceso

¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?

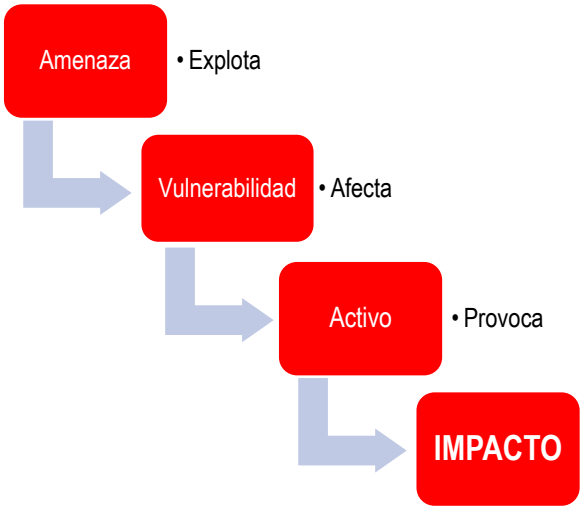
Determinar los posibles efectos por la materialización del riesgo

Nota: En la descripción del riesgo se deben tener en cuenta las respuestas a las preguntas arriba mencionadas.

Se identificarán los siguientes tres (3) riesgos inherentes:

1. •Pérdida de la confidencialidad
2. •Pérdida de la integridad
3. •Pérdida de la disponibilidad

El siguiente diagrama muestra las relaciones entre conceptos:



6.3.1 Identificación de Vulnerabilidades

Acorde a los activos seleccionados para realizar el análisis de riesgo definidos según su criticidad (alto – medio), se realiza la identificación de vulnerabilidades. Estas son las fallas o debilidades que tiene un activo. Cuando la amenaza encuentra la vulnerabilidad surge el riesgo. La Vulnerabilidad se asemeja a la causa.

6.3.2 Identificación de Amenazas

Acorde a los activos seleccionados para realizar el análisis de riesgo definidos según su criticidad (alto – medio), se realiza la identificación de amenazas.

Las amenazas tienen el potencial de causar daños a activos tales como información, procesos y sistemas. Pueden ser de origen natural o humano o podrían ser accidentales o deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización.

Para que una vulnerabilidad pueda causar daño es necesario que una amenaza pueda explotar esa debilidad.

6.3.3 Descripción de Consecuencias

Después de realizar la identificación de amenazas y vulnerabilidades, se identifican las posibles consecuencias de la materialización de una amenaza sobre una vulnerabilidad.

6.3.4 Definición de Riesgos

Acorde a la identificación de vulnerabilidades y amenazas sobre los activos seleccionados objeto del análisis de riesgos, se establecen los riesgos de seguridad a los cuales se encuentra expuesta los activos de información.

Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

6.3.5 Probabilidad de ocurrencia

Se mide en términos de la factibilidad o frecuencia con el riesgo se podría llegar a materializar, teniendo en cuenta la presencia y exposición ante factores internos y externos.

6.3.6 Nivel de Impacto

Por impacto se entienden las consecuencias que puede ocasionar al Instituto la materialización del riesgo y será determinado por un criterio cualitativo y/o cuantitativo.

Las entidades públicas deben identificar y reporten a las instancias y autoridades respectivas en el Gobierno nacional si poseen ICC (Infraestructuras Críticas Cibernéticas). Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios:

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL

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

6.3.7 Valoración del Riesgo

El riesgo inherente es el nivel de exposición presente en ausencia de controles, no se toman en cuenta los controles existes en el Instituto.

La valoración de los riesgos en términos de probabilidad e impacto de ocurrencia se obtiene de aplicar la siguiente ecuación:

Riesgo Inherente= Probabilidad * Impacto

6.4 Plan de Tratamiento

Se debe definir un plan de tratamiento y gestión de los riesgos asociados a los activos de información, el cual tendrá como alcance diseñar y documentar las acciones de mejora que permitan controlar y disminuir los riesgos de seguridad a los que están expuestos los activos de información.Identificación de Controles

6.4.1.1 Controles Actuales

Por cada riesgo inherente identificado, se deben establecer los controles asociados. Así mismo, se determinan las cualidades y características de cada control, que tienen la posibilidad de disminuir el nivel de riesgo, desplazarlas a una zona de riesgo menor a la inherente y determinar si definitivamente es aceptable o no.

7. 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

El tratamiento del riesgo consiste en seleccionar e implementar opciones para abordar el riesgo. La selección de las opciones más apropiadas para el tratamiento del riesgo implica hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos, esfuerzo o desventajas de la implementación.

9. SEGUIMIENTO Y REVISIÓN

El seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas

El seguimiento y la revisión deberían tener lugar en todas etapas del proceso. El seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.

10. REGISTRO E INFORME

La gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados.

11. CAPACITACIÓN

El Plan de Capacitación se llevará de acuerdo al “Plan de Sensibilización para la Seguridad de la Información y Ciberseguridad” el cual forma parte del “Modelo de Seguridad de la Información y Ciberseguridad”.