PLAN DE TRATAMIENTOS DE RIESGOS SEGURIDAD DE LA INFORMACIÓN 2023-2024

Sistema de Gestión de Seguridad de la Información
Secretaría de Educación Del Distrito

Vigencia 2024

Tabla de Contenido

Índice de Tablas

GLOSARIO

ACTIVOS: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

ACTIVO DE INFORMACIÓN: bien de la entidad (representado en su información y datos) que tiene valor para los procesos de negocio, independientemente de su ubicación; puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.

AMENAZAS: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

ANÁLISIS DE RIESGOS: uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

DISPONIBILIDAD: la disponibilidad consiste en asegurarse que los usuarios autorizados tengan acceso a la información y a los sistemas de apoyo, cuando se requiera, se trata de la propiedad de ser accesible y utilizable, bajo solicitud por una entidad autorizada.

CONTINUIDAD: la continuidad es el proceso de establecer por adelantado, las capacidades necesarias para evitar o mitigar el impacto de un acontecimiento que provoca la interrupción de las operaciones en una o más procesos.

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

CONTROL: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

CONTROL DE ACCESO: una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.

CRITICIDAD: medida del impacto que tendría la organización debido a una falla de un sistema y que éste no funcione como es requerido.

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

IMPACTO: el coste para la empresa de un incidente (de la escala que sea), que puede o no ser medido en términos estrictamente financieros.

ISO/IEC 27001:2013: norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

MEDIOS DE ALMACENAMIENTO DIGITAL: son todos aquellos dispositivos autorizados por la Secretaría de Educación del Distrito, que permiten el almacenamiento de información, los cuales pueden ingresar o salir de las instalaciones de la entidad con la respectiva autorización. Se incluyen equipos portátiles, teléfonos inteligentes, Ipods, reproductores mp3, memorias USB/SD/Mini-SD, CDs, DVDs, cintas: respaldo y similares. Asimismo, se incluyen correos electrónicos y conexiones por donde pueda ser transportada la información de la Entidad.

MEDIO REMOVIBLE: medio que permite llevar o transportar información desde un computador a otro. Los medios removibles incluyen cintas, diskettes, discos duros removibles, CDs, DVDs, unidades de almacenamiento USB.

PROCEDIMIENTO: los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

RIESGO: efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo.

SENSIBILIDAD: nivel de impacto que una divulgación no autorizada podría generar.

SERVICIO: es cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

1. JUSTIFICACIÓN

La Secretaría de Educación del Distrito es una entidad que se encarga de dirigir, organizar y planificar el servicio educativo de conformidad con las disposiciones constitucionales, legales y los fines de la educación establecidos en las leyes que regulan el servicio público educativo, en condiciones de calidad, pertinencia, equidad, eficiencia, y efectividad.

La información que se maneja es de carácter confidencial y amparado por la ley 1098 del 2006, la cual en sus artículos tiene por finalidad "garantizar a los niños, a las niñas y a los adolescentes su pleno y armonioso desarrollo para que crezcan en el seno de la familia y de la comunidad, en un ambiente de felicidad, amor y comprensión. Prevaleciendo el reconocimiento a la igualdad y la dignidad humana, sin discriminación alguna".

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema deGestión de Seguridad de la Información de la SED, el cual busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC a través de su plan de acción 2024, ha establecido como meta el tratamiento de los riesgos de seguridad de la información aplicado al proceso Gestión de Tecnologías de Información y Comunicaciones, para ello sea apoyado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas Vr. 5[1].

En la vigencia 2021, se definió la metodología para el tratamiento de riesgos de seguridad y privacidad de la información, de acuerdo con los nuevos lineamientos para la gestión del riesgo de seguridad digital en entidades públicas, dispuesto por el Departamento Administrativo de la Función Pública.

2. METODOLOGIA

La metodología empleada para el análisis de riesgo es la aprobada por la SED mediante el documento Metodología de Administración para la gestión de los Riesgos de Seguridad Digital con fecha de resolución 5-24/Dic/2021, la cual se basa en la guía METODOLOGÍA DE ADMINISTRACIÓN PARA LA GESTIÓN DE LOS RIESGOS DE SEGURIDAD DIGITAL [2], entregada por la Alta consejería de las TIC del 2018, cuyo objetivo es "Estructurar un proceso de gestión de riesgos de seguridad digital -SD-, de acuerdo con el Modelo de Gestión de Riesgos de Seguridad Digital - MGRSD.".

[1] https://gobiernodigital.mintic.gov.co/692/articles-82062_recurso_1.pdf

[2] https://sig.educacionbogota.edu.co/Isolucion/Administracion/frmFrameSet.aspx?Ruta=Li4vRnJhbWVTZXRBcnRpY3Vsby5hc3A/UGFnaW5hPUJhbmNvQ29ub2NpbWllbnRvNFNFRFByby8xLzExYjk1NmJiMmI4NjRkMjRiOTA3ZGNlNDIyNTA5NWFmLzExYjk1NmJiMmI4NjRkMjRiOTA3ZGNlNDIyNTA5NWFmLmFzcCZJREFSVElDVUxPPTUwNDU=

3. OBJETIVO

Mejorar la comprensión de la organización y ampliado su visión sobre su perfil y apetito de riesgo, aclarar el pensamiento sobre la naturaleza y el impacto de los riesgos, y mejorar el modelo de evaluación de riesgos de la organización.

4. ALCANCE

El plan de manejo de riesgos de seguridad digital contempla los procesos del mapa de procesos de la SED, en concordancia con el alcance del Modelo de Seguridad y Privacidad de la Información, habilitador transversal de la Política de Gobierno Digital expedida por el MINTIC.

5. PLAN DE GESTION DE RIESGOS DE SEGURIDAD DIGITAL

La Secretaria de Educación del Distrito establece el Plan de Gestión de Riesgos de Seguridad Digital mediante el cual se identificará las amenazas, las vulnerabilidades, el impacto y el nivel de riesgo asociados a los procesos de la entidad, con relación a la valoración de sus activos de información para determinar el tratamiento de sus riesgos según nivel de criticidad establecido.

5.1. Valoración de riegos

Durante la valoración inicial de activos, con la asesoría de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC se describió el riesgo de forma cualitativa y/o cuantitativa, se determinó el nivel de exposición de los activos de información, e identificación de las causales de riesgo que existen (o que podrían existir), se identifica el impacto que podría generar la materialización de cada riesgo, las consecuencias potenciales, y finalmente se priorizan para identificar o proponer el tratamiento de riesgos y su clasificación según los criterios de evaluación determinados por la entidad.

La OTIC recopila y consolida esta información en la matriz de Gestión de Riesgos de Seguridad Digital.

A continuación, se describe el detalle de las fases que comprende realizar una adecuada valoración de riesgos:

5.2. Identificación de riesgos inherentes de seguridad digital

Como lo indica la Guía para la Administración del Riesgo en la Gestión, Corrupción

y Seguridad Digital. Diseño de Controles en Entidades Públicas[3] emitida por el DAFP, para efectos del presente modelo se podrá 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 de la entidad o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

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. Estos controles deben tomar como base el Anexo A de la Norma ISO/IEC 27001:2013.

5.3. 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.

- **N (**Desastres naturales)
- **I** (De origen Industrial)
- **EI** (Errores y Fallos no Intencionados).
- **AI** (Ataques Intencionados).
- **NI** (Desastres Naturales e Industriales).

Este análisis arroja como resultado la tabla definición de amenazas, en la cual se han clasificado las amenazas que podrían emplear las vulnerabilidades ya conocidas, que afectan el funcionamiento o disponibilidad de los activos de información.

En este cuadro, se realiza la descripción de las amenazas identificadas, a través de los siguientes ID, los cuales se han definido en la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos de Margerit versión 3.0.

[3] https://www.funcionpublica.gov.co/documents/28587410/38054865/2021-01-20_Guia_administracion_riesgos_f.pdf/6351b4f1-2299-8b6e-70b7-f99f6dd4c59a?t=1611257075079

Tabla 1 Definición de amenazas

Tipo de Amenaza	ID	Amenaza	Descripción
Desastres naturales (Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.)	N01	Fuego	incendios: posibilidad de que el fuego acabe con recursos del sistema.
	N02	Daños por agua	inundaciones: posibilidad de que el agua acabe con recursos del sistema.
	N04	Pandemia	Incidentes que pueden ser causados por afectaciones de índole médico y que afectan la disponibilidad del personal y prestación de servicios.
	N*	Desastres naturales	otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ... Se excluyen desastres específicos tales como incendios (ver [N.1]) e inundaciones (ver [N.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.
De origen industrial (Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.)	I01	Fuego	incendios: posibilidad de que el fuego acabe con recursos del sistema.
	I02	Daños por agua	inundaciones: posibilidad de que el agua acabe con recursos del sistema.
	I*	Desastres industriales	otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.18], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.
	I03	Contaminación mecánica	vibraciones, polvo, suciedad.
	I04	Contaminación electromagnética	interferencias de radio, campos magnéticos, luz ultravioleta.
	I05	Avería de origen físico o lógico	fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
	I06	Corte del suministro eléctrico	cese de la alimentación de potencia
	I07	Condiciones inadecuadas de temperatura o humedad	deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.
	I08	Fallo de servicios de comunicaciones	cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.
	I09	Interrupción de otros servicios esenciales	otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tener, refrigerante.
	I10	Degradación de los soportes de almacenamiento de la información	como consecuencia del paso del tiempo

Tipo de Amenaza	ID	Amenaza	Descripción
	I11	Emanaciones electromagnéticas	hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés "Transiten Electromagnética Pulse Standard").
Errores y fallos no intencionados (Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.)	E01	Errores de los usuarios	equivocaciones de las personas cuando usan los servicios, datos, etc.
	E02	Errores del administrador	equivocaciones de personas con responsabilidades de instalación y operación
	E03	Errores de monitorización (log)	inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos.
	E04	Errores de configuración	introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
	E05	Deficiencias en la organización	cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, incumplimientos contractuales, etc.
	E06	Difusión de software dañino	propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
	E07	Errores de [re-]encaminamiento	envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.
	E08	Escapes de información	la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.
	E09	Alteración accidental de la información	alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
	E10	Destrucción de información (accidental)	pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
	E11	Vulnerabilidades de los programas (software)	defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
	E12	Errores de mantenimiento, actualización de programas (software)	defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
	E13	Errores de mantenimiento, actualización de equipos (hardware)	defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.

Tipo de Amenaza	ID	Amenaza	Descripción
	E14	Caída del sistema por agotamiento de recursos	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
	E15	Pérdida de equipos	la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
	E16	Falta de concientización del personal	un manejo inconsciente de seguridad de la información causara riesgos en el manejo y administración de los activos de información.
	E17	Incumplimiento en la disponibilidad del personal	Ausencia de personal adecuado para el cumplimiento de actividades y funciones específicas y acordes a las necesidades del negocio.
Ataques intencionados (Fallos deliberados causados por las personas. La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.)	A01	Manipulación de los registros de actividad (log)	Manipulación de los registros de actividad (log)
	A02	Manipulación de la configuración	prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
	A03	Suplantación de la identidad del usuario	cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.
	A04	Abuso de privilegios de acceso	cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
	A05	Uso no previsto	utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
	A06	Difusión de software dañino	propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
	A07	[Re-]encaminamiento de mensajes	envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.
	A08	Acceso no autorizado	el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
	A09	Análisis de tráfico	el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.

Tipo de Amenaza	ID	Amenaza	Descripción
	A10	Repudio	negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.
	A11	Interceptación de información (escucha)	el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
	A12	Modificación deliberada de la información	alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
	A13	Destrucción de información (Intencional)	eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
	A14	Divulgación de información	revelación de información.
	A15	Manipulación de programas	alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
	A16	Manipulación de los equipos	alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
	A17	Denegación de servicio	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
	A18	Robo	la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
	A19	Ataque destructivo	vandalismo, terrorismo, acción militar, Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.
	A20	Ocupación enemiga	cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.
	A21	Extorsión	presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
	A22	Ingeniería social (picaresca)	abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

5.4. Identificación de Activos de información

Para el proceso de levantamiento de los activos de información, relacionados con el proceso de Gestión de Tecnologías de Información y Comunicaciones, se ha tomado el inventario de sistemas de información de la entidad, que se detallan en el cuadro activos de información. Ver Anexo N.2 Activos de Información

5.5. Determinar la criticidad del activo

Se realiza la valoración de los activos de información del proceso Gestión de Tecnologías de Información y Comunicaciones, lo cual permitirá evaluar el nivel de protección que debe tener cada activo, para ello es necesario dar un valor dependiendo del nivel de importancia para la organización.

Esta clasificación se realizará bajo los criterios de confidencialidad, integridad y disponibilidad, definidos en el cuadro criterios de clasificación de activos.

Tabla 2 Criterios de clasificación de activos

Valor	Nivel	Confidencialidad	Integridad	Disponibilidad
1	BAJA	El acceso no autorizado al activo de información y a la información que este gestiona impacta negativamente de manera leve al proceso evaluado.	La pérdida de la exactitud y el estado completo del activo de información y la información que este gestiona impacta negativamente de manera leve al proceso evaluado.	La ausencia del activo de información y la información que este gestiona impacta negativamente de manera leve al proceso evaluado.
2	MEDIA	El acceso no autorizado al activo de información y a la información que este gestiona impacta negativamente al proceso evaluado.	La pérdida de la exactitud y el estado completo del activo de información y la información que este gestiona impacta negativamente al proceso evaluado.	La ausencia del activo de información y la información que este gestiona impacta negativamente al proceso evaluado.
3	ALTA	El acceso no autorizado al activo de información y a la información que este gestiona impacta negativamente a la entidad.	La pérdida de la exactitud y el estado completo del activo de información y la información que este gestiona impacta negativamente a la entidad.	La ausencia del activo de información y la información que este gestiona impacta negativamente a la entidad.

5.6. Clasificación de activos

Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red, servicios, intangibles, personas e instalaciones, entre otros.

El siguiente cuadro valoración de activos refleja el nivel de valoración dado a cada uno de los activos identificados de acuerdo con los pilares de seguridad de la información valorados. Ver Anexo N° 3 Valoración de activos.

6. ANALISIS DE RIESGOS

Ante una amenaza potencial podemos ahora establecer un análisis con base en los parámetros de la frecuencia y el valor de la vulnerabilidad. La probabilidad con la

cual cada amenaza afectará a cada uno de los activos, y al mismo tiempo el impacto que este generará sobre los mismos.

6.1. Definición de niveles de evaluación de impacto

Para esta actividad se han definido parámetros de evaluación acordes a lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. Octubre 2020, los siguientes parámetros fueron tomados como base de clasificación.

- **Nivel Cualitativo**: es el nivel asignado a cada valor de impacto de acuerdo con la afectación financiera.
- **Nivel Cuantitativo:** define los parámetros de medición de impacto.
- **Criterios de clasificación de impacto:** define los parámetros que se tuvieron en cuenta como criterios para clasificación los mismos.

Tabla 4 Niveles de impacto

Nivel cualitativo	Nivel cuantitativo	Criterios de clasificación de impacto			
		Financiero	**Continuidad**	**Imagen**	**Legal**
		La pérdida de ingresos directa y los costos u otros gastos financieros indirectos que se generarían para la entidad.	Tiempo en que se ve afectada la operación de los procesos de la entidad.	Afectación sobre la imagen y reputación de la entidad.	Emisión de resoluciones administrativas y/o judiciales por el incumplimiento de normas, regulaciones u obligaciones.
Insignificante	**1**	Si el hecho llegara a presentarse, la entidad no tendría consecuencias económicas que impacten el funcionamiento, por tanto se asumirán las perdidas.	Si el hecho llegara a presentarse, el proceso de la entidad no se vería afectado en su continuidad.	Si el hecho llegara a presentarse, tendría consecuencias o efectos sobre un grupo de funcionarios de manera interna.	Si el hecho llegara a presentarse, la entidad tendría multas.
Menor	**2**	Si el hecho llegara a presentarse, la entidad tendría bajas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la entidad se vería afectado en su continuidad de manera mínima.	Si el hecho llegara a presentarse, tendría un impacto leve en la entidad que sería reparable a corto plazo	Si el hecho llegara a presentarse, la entidad tendría demandas.
Moderado	**3**	Si el hecho llegara a presentarse, la entidad tendría medianas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la entidad se vería afectado en su continuidad de manera moderada.	Si el hecho llegara a presentarse, tendría un impacto medio en la entidad de manera local.	Si el hecho llegara a presentarse, la entidad tendría una investigación disciplinaria.

Nivel cualitativo	Nivel cuantitativo	Criterios de clasificación de impacto			
		Financiero	**Continuidad**	**Imagen**	**Legal**
		La pérdida de ingresos directa y los costos u otros gastos financieros indirectos que se generarían para la entidad.	Tiempo en que se ve afectada la operación de los procesos de la entidad.	Afectación sobre la imagen y reputación de la entidad.	Emisión de resoluciones administrativas y/o judiciales por el incumplimiento de normas, regulaciones u obligaciones.
Mayor	**4**	Si el hecho llegara a presentarse, la entidad tendría altas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la entidad se vería afectado en su continuidad de manera considerable interrumpiendo periódicamente el proceso y otros.	Si el hecho llegara a presentarse, tendría un impacto alto en la entidad a nivel gremial.	Si el hecho llegara a presentarse, la entidad tendría una investigación fiscal.
Catastrófico	**5**	Si el hecho llegara a presentarse, la entidad tendría nefastas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la entidad se vería afectado en su continuidad de manera total.	Si el hecho llegara a presentarse, tendría un impacto catastrófico en la entidad a nivel nacional/ internacional.	Si el hecho llegara a presentarse, la entidad tendría sanciones legales. Podría generar el cierre definitivo de la entidad.

6.2. Determinación de la probabilidad

Los niveles de probabilidad definidos significan la posibilidad de materialización de un riesgo sobre determinado activo en un tiempo específico, estos al igual que el punto 5.1 fueron definidos con base en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. Octubre 2020.

Tabla 5 Niveles de probabilidad

Nivel de Probabilidad		Descripción
1	**Raro**	El riesgo ocurre rara vez en la entidad.
2	**Improbable**	El riesgo ocurre en ocasiones especificas en la entidad.
3	**Posible**	El riesgo ocurre con cierta periodicidad en la entidad.
4	**Probable**	El riesgo ocurre frecuentemente en la entidad.
5	**Casi Seguro**	El riesgo ocurre inminentemente en la entidad.

6.3. Identificación de amenazas por activo

Se realiza la valoración de las amenazas que permita evaluar el grado de impacto al activo por medio de los criterios definidos en el cuadro Criterios de clasificación de amenazas.

Tabla 6 Criterios de clasificación de amenazas

Niveles de Clasificación	Impacto (consecuencias) Cualitativo
Catastrófico	• Interrupción de las Operaciones de la entidad por más de cinco (5) días. • Intervención por parte de un ente de control o un ente regulador. Pérdida de información crítica para la entidad que no se puede recuperar. Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. • Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
Mayor	• Interrupción de las Operaciones de la entidad por más de dos (2) días. • Perdida de información crítica que puede ser recuperada de forma parcial o incompleta. • Sanción por parte de entes de control u otro ente regulador. Incumplimiento en la meta y objetivos institucionales afectando el cumplimiento en las metas de gobierno. • Imagen institucional afectada en el orden nacional o regional por incumplimiento en la presentación del servicio a los usuarios o ciudadanos.
Moderado	• Interrupción de las operaciones de la entidad por un (1) día. Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. • Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. • Reproceso de actividades y aumento de carga operativa. Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. • Investigaciones penales fiscales o disciplinarias.
Menor	• Interrupción de las operaciones de la entidad por algunas horas. • Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
Insignificante	• No hay interrupción en las operaciones de la entidad. • No se generan sanciones económicas o administrativas. • No se afecta la imagen institucional de forma significativa.

Luego, se realiza la identificación de activos y amenazas que pueden impactar su funcionamiento, esto se realiza dependiendo de su valor de impacto y probabilidad. Ver Anexo N° 3. Valoración de activos.

6.4. Evaluación de riesgos

Una vez que se ha determinado el valor de riesgo para cada amenaza, que puede afectar a un activo de información, se debe tomar en primer lugar la definición de los criterios aceptables del riesgo. En otras palabras, se tiene que designar qué niveles de riesgos son asumibles y cuales deberán tomar medidas. Para tal efecto se han definido 4 niveles de riesgo para establecer los criterios de tratamiento o aceptación de riesgos según las puntuaciones posibles que se determinan en la tabla Criterios de clasificación de riesgo.

Tabla 7 Criterios de clasificación de riesgo

Niveles de riesgo	Respuesta a los riesgos	Descripción
Bajo	**Asumir el riesgo**	El nivel de riesgo es aceptable y se encuentra controlado en la entidad. Los riesgos en este nivel se deben revisar periódicamente.
Moderado	**Asumir el riesgo**	El nivel de riesgo es moderado de acuerdo con los criterios de aceptación de la entidad. Los riesgos en este nivel deben ser monitoreados para identificar oportunamente los cambios en su valoración. El riesgo ocurre rara vez en la entidad.
Alto	**Mitigar el riesgo, Evitar, Compartir**	El nivel del riesgo es alto, por lo que es necesario implementar controles en la entidad para mitigar, evitar o compartir el riesgo y llevar a niveles aceptables.
Extremo	**Mitigar el riesgo, Evitar, Compartir**	El nivel del riesgo es extremo, por lo que es necesario implementar controles en la entidad para mitigar, evitar o compartir el riesgo y llevar a niveles aceptables.

Con base en los hallazgos del análisis de riesgos, el siguiente paso en el proceso es identificar las medidas que buscan disminuir los diversos niveles de riesgo. Estos se denominan dentro de la norma ISO/IEC 27001:2013 como controles de riesgos para la seguridad de la información.

6.5. Mapa de riesgos

De acuerdo con los resultados obtenidos y empleando la fórmula para valoración del riesgo la cual es dada de la siguiente manera (Riesgo = Impacto x probabilidad), y según formato para el manejo del mapa de riesgos de seguridad digital. Los resultados obtenidos se representan en un mapa de calor, con el análisis de la probabilidad e impacto que tienen las amenazas identificadas para cada uno de los activos; gráfico en el cual, se representan las zonas de riesgo y se asume una posición de tratamiento. Ver Anexo 4°. Mapa General de calor

Zona de riesgo Baja: Asumir el riesgo
Zona de riesgo Moderada: Asumir el riesgo, Reducir el riesgo
Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir
Zona de riesgo Extrema: Reducir el riesgo, Evitar, Compartir o Transferir

Basado en este análisis para los activos de información, desde la OTIC se realizarán mesas de trabajo con los líderes de proceso, para socializar la metodología con las áreas responsables de los procesos de la SED, para que, de acuerdo con la valoración de activos, efectúen un análisis de las amenazas detectadas en sus activos, identifique el nivel de riesgo y se establezcan controles para su tratamiento.

7. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

Una vez identificado los activos importantes desde el proceso de Gestión de Tecnologías de Información y comunicaciones, y realizado el análisis de riesgo para cada uno de los activos identificados por proceso, se ha diseña un plan de tratamiento de riesgos acorde a cada una de las necesidades. Este plan de tratamiento de riesgos le permitirá a la entidad definir cómo tratarlo adecuadamente; el costo/beneficio del tratamiento debe ser un factor decisivo y relevante. Una forma de opciones de tratamiento de riesgo se describe en el siguiente cuadro.

Tabla 8 Opciones tratamiento de riesgo

Costo – beneficio	Opción de tratamiento
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo.
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo.	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero.
El costo y el tiempo del tratamiento es adecuado a los beneficios.	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto.
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Asumir** el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa.

7.1. Aplicación de controles

Los riesgos inherentes se han ubicado en las zonas de riesgo que requieran tratamiento; sobre los cuales, se establecen los controles para garantizar una reducción hasta un nivel aceptable para la SED. Con el fin de verificar esta eficiencia se debe realizar un monitoreo continuo y periódico para establecer la eficacia puesto que estos pueden producir resultados inesperados que deberán ser corregidos y la SED pueda tomar la decisión de aceptar, mitigar, transferir o evitar. Ver Anexo N°5. Tabla Definición de Controles.

7.2. Seguimiento, Monitoreo y Control

El seguimiento de los controles planteados para cada uno de los riesgos de seguridad digital identificados se realizará por el líder de cada uno de los procesos, como primera línea de defensa, en razón a que la ubicación de los riesgos de seguridad digital después de controles debe estar en los niveles bajo y moderado o se deben replantear los controles.

La OTIC realizará el monitoreo de los seguimientos y los cambios que se puedan producir en los diferentes riesgos y los factores que identifiquen los procesos (activos, vulnerabilidades, amenazas, etc.), de manera semestral, y realizará modificaciones o adiciones a tiempo, según enfoque de la metodología adoptado y dependiendo de los cambios que sean identificados e informados por sus responsables. Estos cambios deben ser solicitados por el líder de cada proceso,

como segunda línea de defensa.

La evaluación y control al mapa de riesgos de Seguridad Digital de la SED, lo realizará la Oficina de Control Interno, como tercera línea de defensa, en los tiempos que sean definidos desde la Política de Administración de Riesgos que establece la Oficina Asesora de Planeación.

RESPONSABLE POR ETAPA /LINEA DE DEFENSA	ACTIVIDADES	PERIODO DE EABORACION / REPORTE	
RESPONSABLE ELABORACION **Primera Línea de defensa** **Líder y responsable de los procesos**	1. Elaboración / Actualización Mapa de Riesgos de Seguridad Digital: Se identifica el Riesgo de Seguridad Digital (según Contexto Estratégico, Valoración de activos de información y de riesgos de seguridad digital)	Periodo de elaboración: Anual y durante el primer semestre.	
	2. Seguimiento de riesgos de Seguridad Digital y reporte a OTIC	**Periodo de seguimiento** 1. Marzo - Junio 2. Julio a Diciembre	**Fecha Reporte** 1.22 de julio 2.20 de enero
RESPONSABLE MONITOREO **Segunda Línea de defensa** **OTIC – Líder de la Política de Seguridad Digital**	1. Monitoreo a la elaboración del mapa de riesgos de seguridad digital elaborado por líderes de procesos	**Primer monitoreo:** 30 /07/2024 **Segundo monitoreo:** 31/01/2025	
RESPONSABLE DE EVALUACION Y CONTROL **Tercera Línea de defensa** **Oficina de Control Interno**	1. Revisar que se hayan identificado los riesgos significativos de seguridad digital que pueden afectar el cumplimiento de los objetivos de los procesos 2. Hacer seguimiento a las actividades del control establecidas para mitigar riesgos de seguridad digital de los procesos de la SED.	Anual según cronograma definido por la OCI para el seguimiento de la política de Administración del Riesgos de la SED	

Firma:

Ricardo Abad Chacón Ibarra
Jefe Oficina de Tecnología de la información y las Comunicaciones - OTIC

Elaborado: Juan Carlos Parra Moreno
Profesional Contratista Oficina OTIC

Revisado: Gubileinaya Ramírez Beltrán
Profesional Especializado Oficina OTIC