PLAN DE TRATAMIENTOS DE RIESGOS SEGURIDAD DE LA INFORMACIÓN

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

2023

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 entidad a través del plan de acción 2023, 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 2020, se definió la metodología para el tratamiento de riesgos de seguridad y privacidad de la información, en su anexo 4. Se establecen los nuevos lineamientos para la gestión del riesgo de seguridad digital en entidades públicas, dispuesto por el Departamento Administrativo de la Función Pública.

1 https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?version=1.10&t=1611247032238&download=true

2. METODOLOGIA

La metodología empleada para el análisis de riesgo es la establecida por el Departamento Administrativo de la Función Pública a través de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de igual manera el instructivo para valoración de los activos de información en la SED.

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 presente plan de riesgos tiene alcance para el proceso de Gestión de Tecnologías de Información y Comunicaciones, 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. VALORACION DEL RIESGO

5.1. Valoración de riegos

Durante la valoración, los procesos con la asesoría de la Oficina Administrativa de OTIC describen de forma cualitativa y/o cuantitativa el riesgo, determino el nivel de exposición de los activos de información, e identifican las causales de riesgo que existen (o que podrían existir), identifican 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[2] emitida por el

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

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.

-Errores y fallos no intencionados

- Respaldo lógico

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.

- **EI** (Errores y Fallos no Intencionados).
- **AI** (Ataques Intencionados).
- **NI** (Desastres Naturales e Industriales).

Tabla 1 Definición de amenazas

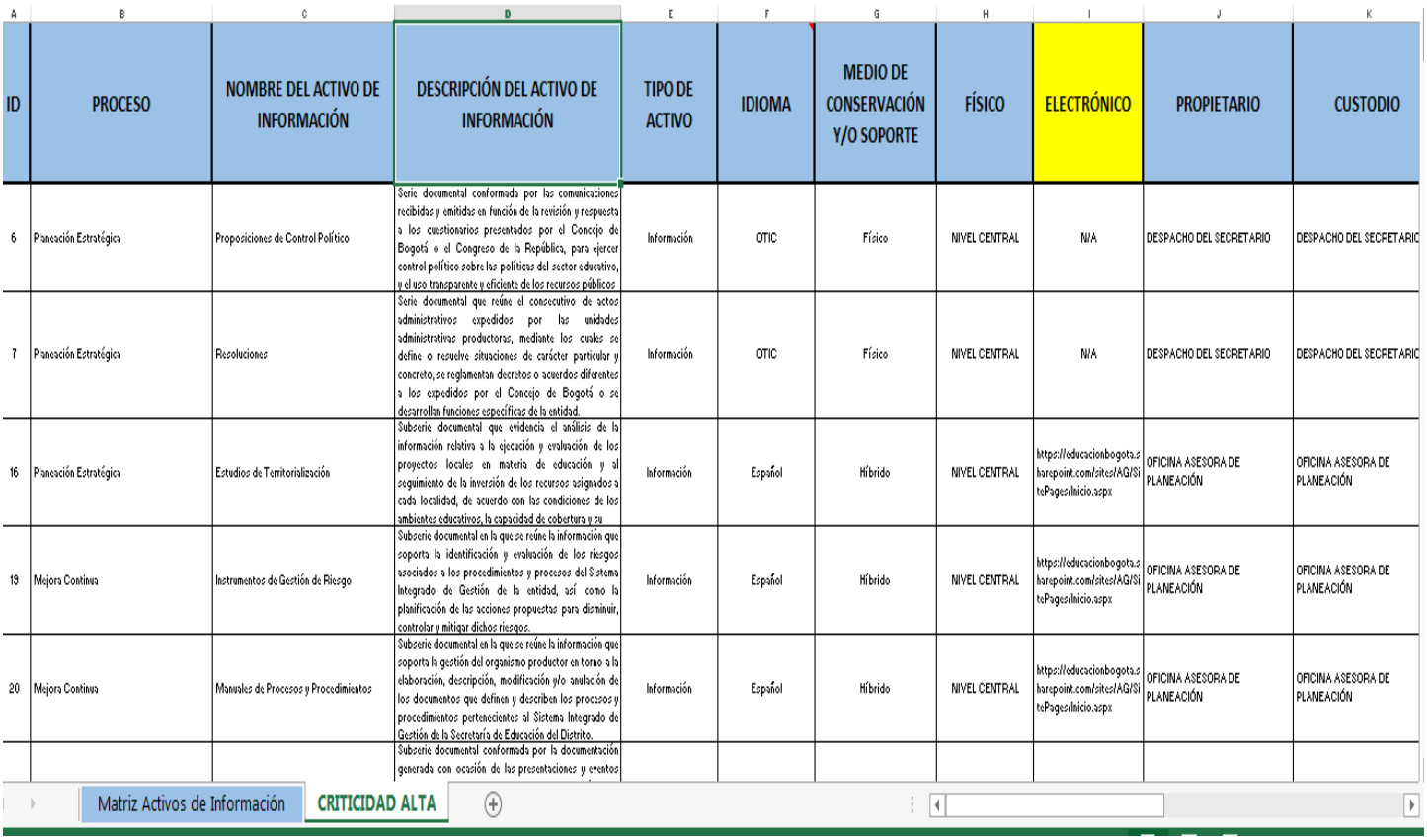
Ítem	Amenaza	Definición
EI01	Incumplimiento de los procedimientos en los Sistemas de Información	Ante la posibilidad de incumplir con los procedimientos referentes a los Sistemas de Información, se hace necesario que el Recurso Humano se encuentre debidamente capacitado para el manejo de los diferentes Sistemas de Información de la Entidad, minimizando vulnerabilidades de los procesos a desarrollar en las herramientas tecnológicas, así como se hace indispensable efectuar entrenamiento cruzado al interior de los procesos para evitar el incumplimiento y retraso de actividades o tareas ante la ausencia del titular.
		De acuerdo a la tendencia cambiante en las tecnologías de información como informáticas, se hace necesario estar a la vanguardia de los nuevos desafíos

Ítem	Amenaza	Definición
AI01	Ataque informático	y lo que esto supone, por esta razón se requiere que el recurso humano se encuentre debidamente capacitado para afrontar posibles ataques informáticos que afecten el desarrollo y la operación de la Entidad, así mismo no se deben escatimar esfuerzos en robustecer las defensas en infraestructura, puesto que ante cualquier situación de ataque, se tendrán consecuencias significativas, de índole legal, económicas, y de información.
NI01	Interrupción de la operación de la(s) plataforma(s) tecnológica(s).	Pueden presentarse situaciones externas que afecten la operación de la plataforma tecnológicas, esto incluye aspectos como desastres naturales, atentados terroristas, así como fallas en el proveedor de servicios informáticos, al interior de la Entidad se pueden observar interrupciones asociadas a los recursos humanos de acuerdo con la manipulación indebida de la infraestructura tecnológica.
AI02	Pérdida, alteración o sustracción de información en medio magnético o físico.	Implementando el Sistema de Seguridad de la Información, el sistema no se convierte en infalible, tampoco se reducen todos los riesgos referentes a Seguridad de la información, gracias a esto la Entidad toma medidas adicionales y controles que fortalezcan y minimicen la posibilidad de pérdida de información, por las causas y consecuencias identificadas al interior de cada proceso las cuales son: - Los permisos y controles de acceso a la información. - La posible carencia de procedimientos de consulta de documentos. - Recurso Humano adecuados o inadecuados para el manejo de información - Posibles intereses a favor de terceros - Mala manipulación de quien recepción los documentos en la Entidad. - Usurpación de contraseñas y privilegios - Ataques informáticos - Personal inconforme al interior de la Entidad o poco compromiso ante las políticas de Seguridad de la Información.
AI03	Alteración, pérdida, divulgación, o uso malintencionado de información sensible para la Entidad	Con el propósito de mantener la Confidencialidad, Integridad y Disponibilidad, se deben evidenciar actividades y labores en la Entidad buscando la protección, alteración y divulgación de información sensible que ha sido clasificada en los activos de información y es transversal para la Entidad. De esta manera mediante la implementación de políticas de usuarios, control de acceso, sensibilización del Manual de políticas de seguridad de la información se busca resguardar la información del uso mal intencionado, incumplimiento de procedimientos, aplicación inadecuada de controles y/o interrupción de los servicios prestados por terceros.

5.4. Identificación de Activos de información

Para el proceso de levantamiento de los activos de información, relacionados con los procesos que se adelantan en las diferentes oficinas y/o dependencias de la SED, sea tomado el inventario de activos de la entidad, que se elaboró conjuntamente con delegados de cada proceso de la SED y que presenta la siguiente información:

Tabla 2 Encabezado Activos de información



ID	PROCESO	NOMBRE DEL ACTIVO DE INFORMACIÓN	DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN	TIPO DE ACTIVO	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FÍSICO	ELECTRÓNICO	PROPIETARIO	CUSTODIO
6	Planeación Estratégica	Proposiciones de Control Político	Serie documental conformada por las comunicaciones recibidas y emitidas en función de la revisión y respuesta a los cuestionarios presentados por el Concejo de Bogotá o el Congreso de la República, para ejercer control político sobre las políticas del sector educativo, y el uso transparente y eficiente de los recursos públicos	Información	OTIC	Físico	NIVEL CENTRAL	N/A	DESPACHO DEL SECRETARIO	DESPACHO DEL SECRETARIO
7	Planeación Estratégica	Resoluciones	Serie documental que reúne el consecutivo de actos administrativos expedidos por las unidades administrativas productoras, mediante los cuales se define o resuelve situaciones de carácter particular y concreto, se reglamentan decretos o acuerdos diferentes a los expedidos por el Concejo de Bogotá o se desarrollan funciones específicas de la entidad.	Información	OTIC	Físico	NIVEL CENTRAL	N/A	DESPACHO DEL SECRETARIO	DESPACHO DEL SECRETARIO
16	Planeación Estratégica	Estudios de Territorialización	Subserie documental que evidencia el análisis de la información relativa a la ejecución y evaluación de los proyectos locales en materia de educación y el seguimiento de la inversión de los recursos asignados a cada localidad, de acuerdo con las condiciones de los ambientes educativos, la capacidad de cobertura y su	Información	Español	Híbrido	NIVEL CENTRAL	https://educacionbogota.sharepoint.com/sites/AGI/SitePages/Inicio.aspx	OFICINA ASESORA DE PLANEACIÓN	OFICINA ASESORA DE PLANEACIÓN
19	Mejora Continua	Instrumentos de Gestión de Riesgo	Subserie documental en la que se reúne la información que soporta la identificación y evaluación de los riesgos asociados a los procedimientos y procesos del Sistema Integrado de Gestión de la entidad, así como la planificación de las acciones propuestas para disminuir, controlar y mitigar dichos riesgos.	Información	Español	Híbrido	NIVEL CENTRAL	https://educacionbogota.sharepoint.com/sites/AGI/SitePages/Inicio.aspx	OFICINA ASESORA DE PLANEACIÓN	OFICINA ASESORA DE PLANEACIÓN
20	Mejora Continua	Manuales de Procesos y Procedimientos	Subserie documental en la que se reúne la información que soporta la gestión del organismo productor en torno a la elaboración, descripción, modificación y/o anulación de los documentos que definen y describen los procesos y procedimientos pertenecientes al Sistema Integrado de Gestión de la Secretaría de Educación del Distrito.	Información	Español	Híbrido	NIVEL CENTRAL	https://educacionbogota.sharepoint.com/sites/AGI/SitePages/Inicio.aspx	OFICINA ASESORA DE PLANEACIÓN	OFICINA ASESORA DE PLANEACIÓN
			Subserie documental conformada por la documentación generada con ocasión de las presentaciones y eventos							

Matriz Activos de Información | CRITICIDAD ALTA

5.5. Determinar la criticidad del activo

Se realiza la valoración de los activos de información conjuntamente con los delegados de cada proceso, 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 3 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.

Los delegados de cada proceso realizan la valoración de cada activo y el equipo de seguridad filtra los activos valorados con criticidad “ALTA” de acuerdo con los pilares de seguridad de la información. El siguiente cuadro valoración de activos refleja el nivel de valoración dado a cada uno de ellos:

Tabla 4 Valoración de activos

ID	CONFIDENCIALIDAD Seleccione entre: (Alta, Media, Baja)	INTEGRIDAD Seleccione entre: (Alta, Media, Baja)	DISPONIBILIDAD Seleccione entre: (Alta, Media, Baja)	CRITICIDAD
6	Baja	Alta	Alta	**ALTA**
7	Baja	Alta	Alta	**ALTA**
16	Baja	Alta	Alta	**ALTA**
19	Baja	Alta	Alta	**ALTA**
20	Baja	Alta	Alta	**ALTA**
21	Baja	Alta	Alta	**ALTA**
22	Baja	Alta	Alta	**ALTA**
26	Media	Alta	Alta	**ALTA**
35	Alta	Alta	Media	**ALTA**
36	Alta	Alta	Media	**ALTA**
39	Alta	Alta	Alta	**ALTA**
44	Alta	Alta	Media	**ALTA**
45	Alta	Alta	Alta	**ALTA**
52	Alta	Alta	Alta	**ALTA**
53	Alta	Alta	Alta	**ALTA**
68	Baja	Alta	Alta	**ALTA**

71	Baja	Alta	Alta	**ALTA**
85	Media	Alta	Alta	**ALTA**
91	Alta	Media	Alta	**ALTA**
92	Media	Alta	Alta	**ALTA**
93	Media	Alta	Alta	**ALTA**
101	Media	Alta	Alta	**ALTA**
115	Media	Alta	Alta	**ALTA**
130	Media	Alta	Alta	**ALTA**
136	Alta	Media	Alta	**ALTA**
137	Media	Alta	Alta	**ALTA**
138	Media	Alta	Alta	**ALTA**
146	Media	Alta	Alta	**ALTA**
160	Media	Alta	Alta	**ALTA**
166	Alta	Media	Alta	**ALTA**
167	Media	Alta	Alta	**ALTA**
168	Media	Alta	Alta	**ALTA**
176	Media	Alta	Alta	**ALTA**
182	Alta	Alta	Alta	**ALTA**
184	Alta	Alta	Media	**ALTA**
185	Alta	Alta	Media	**ALTA**
187	Media	Alta	Alta	**ALTA**
188	Media	Alta	Alta	**ALTA**
205	Media	Alta	Alta	**ALTA**
220	Media	Alta	Alta	**ALTA**
235	Media	Alta	Alta	**ALTA**
250	Media	Alta	Alta	**ALTA**
265	Media	Alta	Alta	**ALTA**
280	Media	Alta	Alta	**ALTA**
295	Media	Alta	Alta	**ALTA**
310	Media	Alta	Alta	**ALTA**
325	Media	Alta	Alta	**ALTA**
336	Alta	Alta	Media	**ALTA**
341	Media	Alta	Alta	**ALTA**
355	Media	Alta	Alta	**ALTA**
361	Media	Alta	Alta	**ALTA**
364	Alta	Alta	Media	**ALTA**
367	Alta	Alta	Media	**ALTA**
368	Alta	Alta	Media	**ALTA**

369	Alta	Alta	Media	**ALTA**
370	Alta	Alta	Media	**ALTA**
399	Baja	Alta	Alta	**ALTA**
400	Alta	Alta	Alta	**ALTA**
409	Baja	Alta	Alta	**ALTA**
410	Baja	Alta	Alta	**ALTA**
411	Baja	Alta	Alta	**ALTA**
412	Baja	Alta	Alta	**ALTA**
413	Baja	Alta	Alta	**ALTA**
414	Baja	Alta	Alta	**ALTA**
415	Baja	Alta	Alta	**ALTA**
416	Baja	Alta	Alta	**ALTA**
422	Baja	Alta	Alta	**ALTA**
423	Baja	Alta	Alta	**ALTA**
424	Baja	Alta	Alta	**ALTA**
425	Baja	Alta	Alta	**ALTA**
426	Baja	Alta	Alta	**ALTA**
427	Baja	Alta	Alta	**ALTA**
428	Baja	Alta	Alta	**ALTA**
430	Baja	Alta	Alta	**ALTA**
431	Baja	Alta	Alta	**ALTA**
437	Baja	Alta	Alta	**ALTA**
442	Baja	Alta	Alta	**ALTA**
444	Baja	Alta	Alta	**ALTA**
445	Baja	Alta	Alta	**ALTA**
446	Baja	Alta	Alta	**ALTA**
449	Media	Alta	Alta	**ALTA**
451	Media	Alta	Alta	**ALTA**
452	Media	Alta	Alta	**ALTA**
453	Media	Alta	Alta	**ALTA**
457	Baja	Alta	Alta	**ALTA**
462	Baja	Alta	Alta	**ALTA**
465	Alta	Alta	Media	**ALTA**
469	Alta	Alta	Alta	**ALTA**
483	Baja	Alta	Alta	**ALTA**
484	Baja	Alta	Alta	**ALTA**
488	Alta	Alta	Media	**ALTA**
490	Alta	Alta	Media	**ALTA**

494	Baja	Alta	Alta	**ALTA**
495	Baja	Alta	Alta	**ALTA**
496	Baja	Alta	Alta	**ALTA**
500	Baja	Alta	Alta	**ALTA**
503	Baja	Alta	Alta	**ALTA**
512	Baja	Alta	Alta	**ALTA**
515	Baja	Alta	Alta	**ALTA**
516	Baja	Alta	Alta	**ALTA**
517	Baja	Alta	Alta	**ALTA**
518	Baja	Alta	Alta	**ALTA**
519	Baja	Alta	Alta	**ALTA**
538	Baja	Alta	Alta	**ALTA**
550	Media	Alta	Alta	**ALTA**
551	Alta	Alta	Alta	**ALTA**
553	Alta	Alta	Media	**ALTA**
558	Alta	Alta	Media	**ALTA**
559	Alta	Alta	Media	**ALTA**
560	Alta	Alta	Media	**ALTA**
571	Alta	Alta	Alta	**ALTA**
575	Baja	Alta	Alta	**ALTA**
578	Baja	Alta	Alta	**ALTA**
579	Baja	Alta	Alta	**ALTA**
580	Baja	Alta	Alta	**ALTA**
581	Baja	Alta	Alta	**ALTA**
582	Baja	Alta	Alta	**ALTA**
583	Baja	Alta	Alta	**ALTA**
589	Baja	Alta	Alta	**ALTA**
590	Baja	Alta	Alta	**ALTA**
591	Baja	Alta	Alta	**ALTA**
592	Baja	Alta	Alta	**ALTA**
593	Alta	Alta	Media	**ALTA**
595	Media	Alta	Alta	**ALTA**
596	Baja	Alta	Alta	**ALTA**
597	Media	Alta	Alta	**ALTA**
598	Alta	Alta	Alta	**ALTA**
599	Alta	Alta	Media	**ALTA**
600	Alta	Alta	Alta	**ALTA**
601	Baja	Alta	Alta	**ALTA**

602	Baja	Alta	Alta	**ALTA**
608	Baja	Alta	Alta	**ALTA**
609	Baja	Alta	Alta	**ALTA**
610	Baja	Alta	Alta	**ALTA**
611	Baja	Alta	Alta	**ALTA**
632	Baja	Alta	Alta	**ALTA**
634	Baja	Alta	Alta	**ALTA**
635	Baja	Alta	Alta	**ALTA**
636	Baja	Alta	Alta	**ALTA**
637	Baja	Alta	Alta	**ALTA**
638	Baja	Alta	Alta	**ALTA**
639	Baja	Alta	Alta	**ALTA**
640	Baja	Alta	Alta	**ALTA**
641	Baja	Alta	Alta	**ALTA**
642	Baja	Alta	Alta	**ALTA**
643	Baja	Alta	Alta	**ALTA**
644	Baja	Alta	Alta	**ALTA**
646	Baja	Alta	Alta	**ALTA**
647	Baja	Alta	Alta	**ALTA**
662	Alta	Alta	Media	**ALTA**
663	Alta	Alta	Media	**ALTA**
664	Alta	Alta	Alta	**ALTA**
668	Alta	Alta	Media	**ALTA**
669	Alta	Alta	Media	**ALTA**
672	Alta	Alta	Media	**ALTA**
673	Alta	Alta	Media	**ALTA**
684	Alta	Alta	Media	**ALTA**
685	Alta	Alta	Alta	**ALTA**
686	Alta	Alta	Alta	**ALTA**
687	Alta	Alta	Alta	**ALTA**
692	Alta	Alta	Alta	**ALTA**
693	Alta	Alta	Alta	**ALTA**
694	Alta	Alta	Alta	**ALTA**
695	Alta	Alta	Alta	**ALTA**
697	Alta	Alta	Alta	**ALTA**
699	Alta	Alta	Alta	**ALTA**
700	Alta	Alta	Alta	**ALTA**
707	Alta	Alta	Alta	**ALTA**

708	Alta	Alta	Alta	**ALTA**
709	Alta	Alta	Alta	**ALTA**
725	Alta	Alta	Media	**ALTA**
730	Alta	Alta	Alta	**ALTA**
740	Alta	Alta	Baja	**ALTA**
741	Alta	Alta	Alta	**ALTA**
743	Alta	Alta	Alta	**ALTA**
744	Alta	Alta	Media	**ALTA**
745	Alta	Alta	Media	**ALTA**
746	Alta	Media	Alta	**ALTA**
755	Alta	Alta	Media	**ALTA**
758	Alta	Alta	Media	**ALTA**
780	Alta	Baja	Alta	**ALTA**
781	Alta	Baja	Alta	**ALTA**
782	Alta	Baja	Alta	**ALTA**
784	Alta	Baja	Alta	**ALTA**
785	Alta	Baja	Alta	**ALTA**
787	Alta	Baja	Alta	**ALTA**
788	Alta	Baja	Alta	**ALTA**
789	Alta	Baja	Alta	**ALTA**
790	Alta	Baja	Alta	**ALTA**
791	Alta	Baja	Alta	**ALTA**
792	Alta	Baja	Alta	**ALTA**
794	Alta	Baja	Alta	**ALTA**
795	Alta	Baja	Alta	**ALTA**
796	Alta	Baja	Alta	**ALTA**
797	Alta	Baja	Alta	**ALTA**
799	Alta	Baja	Alta	**ALTA**
800	Alta	Baja	Alta	**ALTA**
801	Alta	Baja	Alta	**ALTA**
802	Alta	Baja	Alta	**ALTA**
803	Alta	Baja	Alta	**ALTA**
804	Alta	Baja	Alta	**ALTA**
806	Alta	Baja	Alta	**ALTA**
808	Alta	Baja	Alta	**ALTA**
809	Alta	Baja	Alta	**ALTA**
810	Alta	Baja	Alta	**ALTA**
839	Alta	Baja	Alta	**ALTA**

862	Alta	Baja	Alta	**ALTA**
881	Alta	Alta	Alta	**ALTA**
883	Alta	Alta	Media	**ALTA**
884	Alta	Alta	Media	**ALTA**
885	Alta	Alta	Media	**ALTA**
889	Alta	Alta	Media	**ALTA**
891	Alta	Media	Alta	**ALTA**
893	Alta	Alta	Baja	**ALTA**
894	Alta	Media	Alta	**ALTA**
898	Alta	Alta	Media	**ALTA**
902	Media	Alta	Alta	**ALTA**
903	Media	Alta	Alta	**ALTA**
912	Alta	Alta	Alta	**ALTA**
918	Alta	Alta	Alta	**ALTA**

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 5 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 seria 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.
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 6 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 7 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.

Niveles de Clasificación	Impacto (consecuencias) Cualitativo
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.

A continuación, se realiza la identificación de activos y amenazas que pueden impactar su funcionamiento, esto se realiza dependiendo de su valor de impacto y probabilidad, como se aprecia en la tabla valoración activo.

Tabla 8 Valor del riesgo

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
S001	EI01	1	3	3	R01
S001	AI01	2	1	2	R02
S001	NI01	2	2	4	R03
S001	AI02	2	3	6	R04
S001	AI03	2	3	6	R05
S002	EI01	1	3	3	R06
S002	AI01	2	3	6	R07
S002	NI01	2	3	6	R08
S002	AI02	2	2	4	R09
S002	AI03	2	2	4	R10
S003	EI01	2	3	6	R11
S003	AI01	2	3	6	R12
S003	NI01	2	3	6	R13
S003	AI02	2	2	4	R14
S003	AI03	2	2	4	R15
S004	EI01	3	3	9	R16
S004	AI01	3	2	6	R17
S004	NI01	3	3	9	R18

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
S004	AI02	3	1	3	R19
S004	AI03	3	2	6	R20
S005	EI01	1	3	3	R21
S005	AI01	1	2	2	R22
S005	NI01	1	3	3	R23
S005	AI02	1	2	2	R24
S005	AI03	1	2	2	R25
S006	EI01	1	3	3	R26
S006	AI01	1	1	1	R27
S006	NI01	1	2	2	R28
S006	AI02	1	2	2	R29
S006	AI03	1	2	2	R30
S007	EI01	3	3	9	R31
S007	AI01	3	1	3	R32
S007	NI01	3	3	9	R33
S007	AI02	3	2	6	R34
S007	AI03	3	2	6	R35
S008	EI01	1	2	2	R36
S008	AI01	1	1	1	R37
S008	NI01	1	3	3	R38
S008	AI02	1	2	2	R39
S008	AI03	1	2	2	R40
S009	EI01	1	2	2	R41
S009	AI01	1	1	1	R42
S009	NI01	1	3	3	R43
S009	AI02	1	2	2	R44
S009	AI03	1	2	2	R45
S010	EI01	1	2	2	R46
S010	AI01	1	1	1	R47
S010	NI01	1	3	3	R48
S010	AI02	1	2	2	R49
S010	AI03	1	2	2	R50
S011	EI01	1	2	2	R51
S011	AI01	1	1	1	R52
S011	NI01	1	3	3	R53
S011	AI02	1	2	2	R54
S011	AI03	1	2	2	R55
S012	EI01	2	2	4	R56
S012	AI01	2	1	2	R57

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
S012	NI01	2	3	6	R58
S012	AI02	2	2	4	R59
S012	AI03	2	2	4	R60
S013	EI01	1	2	2	R61
S013	AI01	1	1	1	R62
S013	NI01	1	3	3	R63
S013	AI02	1	2	2	R64
S013	AI03	1	2	2	R65
S014	EI01	2	2	4	R66
S014	AI01	2	1	2	R67
S014	NI01	2	3	6	R68
S014	AI02	2	2	4	R69
S014	AI03	2	2	4	R70
S015	EI01	1	2	2	R71
S015	AI01	1	1	1	R72
S015	NI01	1	3	3	R73
S015	AI02	1	2	2	R74
S015	AI03	1	2	2	R75
S016	EI01	1	2	2	R76
S016	AI01	1	1	1	R77
S016	NI01	1	3	3	R78
S016	AI02	1	2	2	R79
S016	AI03	1	2	2	R80
S017	EI01	2	2	4	R81
S017	AI01	2	1	2	R82
S017	NI01	2	3	6	R83
S017	AI02	2	2	4	R84
S017	AI03	2	2	4	R85
S018	EI01	3	2	6	R86
S018	AI01	3	3	9	R87
S018	NI01	3	3	9	R88
S018	AI02	3	3	9	R89
S018	AI03	3	2	6	R90
S019	EI01	2	2	4	R91
S019	AI01	2	1	2	R92
S019	NI01	2	3	6	R93
S019	AI02	2	2	4	R94
S019	AI03	2	2	4	R95
S020	EI01	3	2	6	R96

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
S020	AI01	3	3	9	R97
S020	NI01	3	3	9	R98
S020	AI02	3	2	6	R99
S020	AI03	3	3	9	R100
S021	EI01	2	2	4	R101
S021	AI01	2	1	2	R102
S021	NI01	2	3	6	R103
S021	AI02	2	2	4	R104
S021	AI03	2	2	4	R105
S022	EI01	3	2	6	R106
S022	AI01	3	3	9	R107
S022	NI01	3	3	9	R108
S022	AI02	3	2	6	R109
S022	AI03	3	3	9	R110
S023	EI01	3	2	6	R111
S023	AI01	3	3	9	R112
S023	NI01	3	3	9	R113
S023	AI02	3	2	6	R114
S023	AI03	3	3	9	R115
S024	EI01	2	2	4	R116
S024	AI01	2	1	2	R117
S024	NI01	2	3	6	R118
S024	AI02	2	2	4	R119
S024	AI03	2	2	4	R120
S025	EI01	2	2	4	R121
S025	AI01	2	1	2	R122
S025	NI01	2	3	6	R123
S025	AI02	2	2	4	R124
S025	AI03	2	2	4	R125
S026	EI01	1	2	2	R126
S026	AI01	1	1	1	R127
S026	NI01	1	3	3	R128
S026	AI02	1	2	2	R129
S026	AI03	1	2	2	R130
S027	EI01	1	2	2	R131
S027	AI01	1	1	1	R132
S027	NI01	1	3	3	R133
S027	AI02	1	2	2	R134
S027	AI03	1	2	2	R135

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
S028	EI01	3	2	6	R136
S028	AI01	3	3	9	R137
S028	NI01	3	3	9	R138
S028	AI02	3	2	6	R139
S028	AI03	3	3	9	R140
S029	EI01	2	2	4	R141
S029	AI01	2	1	2	R142
S029	NI01	2	3	6	R143
S029	AI02	2	2	4	R144
S029	AI03	2	2	4	R145
S030	EI01	3	2	6	R146
S030	AI01	3	1	3	R147
S030	NI01	3	3	9	R148
S030	AI02	3	2	6	R149
S030	AI03	3	2	6	R150
S031	EI01	3	2	6	R151
S031	AI01	3	3	9	R152
S031	NI01	3	3	9	R153
S031	AI02	3	2	6	R154
S031	AI03	3	3	9	R155
S032	EI01	2	2	4	R156
S032	AI01	2	1	2	R157
S032	NI01	2	3	6	R158
S032	AI02	2	2	4	R159
S032	AI03	2	2	4	R160
S033	EI01	1	2	2	R161
S033	AI01	1	1	1	R162
S033	NI01	1	3	3	R163
S033	AI02	1	2	2	R164
S033	AI03	1	2	2	R165
S034	EI01	1	2	2	R166
S034	AI01	1	1	1	R167
S034	NI01	1	3	3	R168
S034	AI02	1	2	2	R169
S034	AI03	1	2	2	R170
S035	EI01	3	2	6	R171
S035	AI01	3	3	9	R172
S035	NI01	3	3	9	R173
S035	AI02	3	2	6	R174

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
S035	AI03	3	3	9	R175
S036	EI01	1	2	2	R176
S036	AI01	1	1	1	R177
S036	NI01	1	3	3	R178
S036	AI02	1	2	2	R179
S036	AI03	1	2	2	R180
S037	EI01	1	2	2	R181
S037	AI01	1	1	1	R182
S037	NI01	1	3	3	R183
S037	AI02	1	2	2	R184
S037	AI03	1	2	2	R185
S038	EI01	1	2	2	R186
S038	AI01	1	1	1	R187
S038	NI01	1	3	3	R188
S038	AI02	1	2	2	R189
S038	AI03	1	2	2	R190
S039	EI01	1	2	2	R191
S039	AI01	1	1	1	R192
S039	NI01	1	3	3	R193
S039	AI02	1	2	2	R194
S039	AI03	1	2	2	R195
S040	EI01	1	2	2	R196
S040	AI01	1	1	1	R197
S040	NI01	1	3	3	R198
S040	AI02	1	2	2	R199
S040	AI03	1	2	2	R200
S041	EI01	1	2	2	R201
S041	AI01	1	1	1	R202
S041	NI01	1	3	3	R203
S041	AI02	1	2	2	R204
S041	AI03	1	2	2	R205
S042	EI01	1	2	2	R206
S042	AI01	1	1	1	R207
S042	NI01	1	3	3	R208
S042	AI02	1	2	2	R209
S042	AI03	1	2	2	R210
S043	EI01	1	2	2	R211
S043	AI01	1	1	1	R212
S043	NI01	1	3	3	R213

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
S043	AI02	1	2	2	R214
S043	AI03	1	2	2	R215
S044	EI01	1	2	2	R216
S044	AI01	1	1	1	R217
S044	NI01	1	3	3	R218
S044	AI02	1	2	2	R219
S045	AI03	1	2	2	R220
S045	EI01	3	2	6	R221
S045	AI01	3	1	3	R222
S045	NI01	3	3	9	R223
S045	AI02	3	2	6	R224
S046	AI03	3	2	6	R225
S046	EI01	1	2	2	R226
S046	AI01	1	1	1	R227
S046	NI01	1	3	3	R228
S046	AI02	1	2	2	R229
S046	AI03	1	2	2	R230
S047	EI01	2	2	4	R231
S047	AI01	2	2	4	R232
S047	NI01	2	1	2	R233
S047	AI02	2	3	6	R234
S047	AI03	2	2	4	R235
S048	EI01	3	2	6	R236
S048	AI01	3	2	6	R237
S048	NI01	3	1	3	R238
S048	AI02	3	3	9	R239
S048	AI03	3	2	6	R240
S049	EI01	2	2	4	R241
S049	AI01	2	2	4	R242
S049	NI01	2	1	2	R243
S049	AI02	2	3	6	R244
S049	AI03	2	2	4	R245
S050	EI01	2	2	4	R246
S050	AI01	2	2	4	R247
S050	NI01	2	1	2	R248
S050	AI02	2	3	6	R249
S050	AI03	2	2	4	R250
S051	EI01	1	2	2	R251
S051	AI01	1	2	2	R252

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
S051	NI01	1	1	1	R253
S051	AI02	1	3	3	R254
S051	AI03	1	2	2	R255
S052	EI01	2	2	4	R256
S052	AI01	2	2	4	R257
S052	NI01	2	1	2	R258
S052	AI02	2	3	6	R259
S052	AI03	2	2	4	R260

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 41 tratamiento o aceptación de riesgos según las puntuaciones posibles que se determinan en la tabla Criterios de clasificación de riesgo.

Tabla 9 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. En primer lugar, se debe considerar realizar un

plan urgente para incluir actualizaciones de controles adicionales por encima de los estándares mínimos recomendados por la organización, según sea necesario, para abordar las amenazas específicas y los riesgos asociados que se hayan identificado siempre que se hayan evaluado los costos estimados para implementar dichas medidas.

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). Los resultados obtenidos se representan en el siguiente mapa de calor, con el análisis de la probabilidad e impacto que tienen las amenazas identificadas para cada uno de los activos. (ver cuadro Mapa de calor general), para cada una de las zonas de riesgo se asume una posición de tratamiento de este, de la siguiente manera.

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

Tabla 10 Mapa de calor general

Muy Alta100%					
Alta80%					
Media 60%	R141-R142-R145-R146 R147-R148-R149-R150 R151-R153-R154-R155 R156-R158-R159-R160 R161-R194-R284-R336 R502-R504-R754-R756 R760	R58-R59-R62-R63-R279 R64-R65-R66-R67-R283 R74-R75-R76-R77-R292 R80-R85-R86-R89-R297 R90-R91-R92-R93-R302 R94-R95-R97-R98-R303 R99-R100-R102-R132 R103-R104-R105-R133 R108-R113-R114-R131 R117-R118-R119-R130 R120-R121-R122-R128 R123-R125-R126-R127 R136-R199-R208-R213 R218-R219-R221-R305 R339-R348-R353-R358 R359-R361-R363-R367 R376-R381-R386-R387 R389-R391-R395-R404 R409-R414-R415-R417 R503-R507-R516-R521 R526-R527-R529-R755 R759-R768-R773-R778	R04-R05-R08-R09-R281 R10-R11-R12-R13-R15 R16-R17-R18-R50-R53 R20-R21-R22-R23-R35 R31-R32-R34-R48-R49 R36-R37-R38-R39-R47 R40-R42-R43-R44-R45 R195-R197-R198-R201 R202-R203-R204-R205 R206-R207-R209-R210 R211-R212-R214-R215 R216-R217-R220-R282 R285-R286-R287-R288 R289-R290-R291-R293 R294-R295-R296-R298 R299-R300-R301-R304 R337-R338-R341-R342 R343-R344-R345-R346 R347-R349-R350-R351 R352-R354-R355-R356 R357-R360-R365-R366 R369-R370-R371-R372 R373-R374-R375-R377 R378-R379-R380-R382 R383-R384-R385-R388 R393-R394-R397-R398 R399-R400-R401-R402 R403-R405-R406-R407		

Probabilidad	Baja 40%	R139-R143-R152-R228 R157-R162-R163-R250 R165-R224-R252-R306 R308-R312-R418-R420 R424-R446-R448-R452 R474-R476-R480-R530 R532-R536-R558-R560 R564-R586-R592-R642 R644-R648-R670-R672 R676-R698-R700-R704 R726-R728-R732-R782 R784-R788-R810-R812 R816-R838-R840-R844	R56-R60-R68-R73-R223 R78-R79-R81-R83-R227 R87-R96-R101-R236 R106-R107-R109-R241 R111-R115-R124-R246 R129-R134-R135-R247 R137-R249-R251-R255 R274-R275-R277-R307 R311-R320-R325-R330 R331-R333-R335-R419 R423-R432-R437-R442 R443-R445-R447-R451 R460-R465-R470-R471 R473-R475-R479-R488 R493-R498-R499-R501 R531-R535-R544-R549 R554-R555-R557-R559 R563-R572-R577-R582 R583-R585-R587-R591 R600-R605-R610-R611 R613-R643-R647-R656 R661-R666-R667-R669 R671-R675-R684-R689 R694-R695-R697-R699 R703-R712-R717-R722 R723-R725-R727-R731	R02-R06-R14-R19-R229 R24-R25-R27-R29-R230 R33-R41-R46-R51-R231 R52-R54-R69-R70-R232 R71-R72-R225-R226-R233 R234-R235-R237-R238 R239-R240-R242-R243 R244-R245-R248-R253 R254-R257-R258-R259 R260-R261-R262-R263 R265-R266-R267-R268 R270-R271-R272-R273 R276-R309-R310-R313 R314-R315-R316-R317 R318-R319-R321-R322 R323-R324-R326-R329 R332-R421-R422-R425 R426-R427-R248-R429 R430-R431-R433-R434 R435-R436-R438-R439 R440-R441-R444-R449 R450-R453-R454-R455 R456-R457-R458-R459 R461-R362-R363-R464 R466-R467-R468-R469 R472-R477-R478-R481 R482-R483-R484-R485 R486-R487-R489-R490		
	Muy Baja 20%	R138-R140-R144-R164 R166-R168-R172-R614 R616-R620	R57-R61-R82-R84-R256 R88-R110-R112-R116 R167-R171-R190-R191 R193-R222-R264-R269 R615-R619-R628-R633 R638-R639-R641	R01-R03-R07-R28-R280 R30-R34-R55-R169-R340 R170-R173-R174-R175 R176-R177-R178-R179 R180-R181-R182-R183 R184-R185-R186-R187 R188-R189-R192-R196 R200-R278-R334-R362 R364-R368-R390-R392 R396-R508-R617-R618 R621-R622-R623-R624 R625-R626-R627-R629 R630-R631-R632-R634 R635-R636-R637-R640		
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
		Impacto				

7. PLAN DE TRATAMIENTO DE RIESGOS

Luego de haber identificado los activos importantes en el proceso de Gestión de Tecnologías de Información y comunicaciones y realizado el análisis de riesgo para cada uno de los activos identificados, se ha diseñado un plan de tratamiento de riesgos acorde a cada una de las necesidades. Este plan de tratamiento de riesgos le permitirá a la compañía definir cómo tratarlo adecuadamente; el costo/beneficio del tratamiento debe ser un factor decisivo y relevante para la compañía, tal como se aprecia en el cuadro Opciones tratamiento de riesgo.

Tabla 11 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	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero.

Costo – beneficio	Opción de tratamiento
tratamiento directo.	
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; se deberán tomar las siguientes acciones de acuerdo con los controles que se puedan establecer, todos los riesgos que sean tratados con los controles deben 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 tabla Definición de Controles)

Tabla 12 Definición de controles

Riesgo	Control de la Norma	Estrategia
R01-R06-R11-R16-R21-R26 R31-R36-R41-R46-R51-R56 R61-R66-R71-R76-R81-R86 R91-R96-R101-R106-R111 R116-R121-R126-R131-R136 R141-R146-R151-R156-R161 R166-R171-R176-R181-R186 R191-R196-R201-R206-R211 R216-R221-R226-R231-R241 R246-R251-R256	A.5.1.1 Políticas para la seguridad de la información.	Defina políticas de seguridad de la información claras y alineadas con los objetivos corporativos y cuyo alcance garantice el cumplimiento legal.
	A.12.1.1 Documentación de procedimientos de operación.	Todo cambio desarrollado se debe controlar y documentar de acuerdo con las decisiones o aceptaciones que se presentaron en el comité de cambios.
	A.9.2.2 Gestión de los derechos de acceso asignados a usuarios.	Los administradores de la plataforma deberán tener un compromiso de revisar periódicamente los derechos de acceso de los usuarios, para validar que no se hubiera alterado ningún permiso.
	A.12.1.1 Documentación de procedimientos de operación.	Todo cambio desarrollado se debe controlar y documentar de acuerdo con las decisiones o aceptaciones que se presentaron en el comité de cambios.
	A.6.1.1 Roles y responsabilidades para la seguridad de la información.	Configure los sistemas para que generen una entrada de registro y una alerta cuando se agregue o elimine una cuenta a cualquier grupo que tenga asignados privilegios administrativos: * Configure los sistemas para generar una entrada de registro y una alerta de inicios de sesión fallidos en una cuenta administrativa. * Regularmente, revise los registros para identificar anomalías o eventos anormales.
R02-R07-R12-R17-R22-R27 R32-R37-R42-R47-R52-R57	A.5.1.1 Políticas para la seguridad de la información.	Defina políticas de seguridad de la información claras y alineadas con los objetivos corporativos y cuyo alcance garantice el cumplimiento legal.

Riesgo	Control de la Norma	Estrategia
R62-R67-R72-R77-R82-R87 R92-R97-R102-R107-R112 R117-R122-R127-R132-R137 R142-R147-R152-R157-R162 R167-R172-R177-R182-R187 R192-R197-R202-R207-R212 R217-R222-R227-R232-R237 R242-R247-R252-R257	A.9.4.1 Restricción del acceso a la información.	Hacer cumplir el registro de auditoría detallado para acceder a datos confidenciales o cambios en datos confidenciales (utilizando herramientas como File Integrity Monitoring o Información de seguridad y monitoreo de eventos).
	A.9.2 Gestión de los derechos de acceso asignados a usuarios.	Los administradores de la plataforma deberán tener un compromiso de revisar periódicamente los derechos de acceso de los usuarios, para validar que no se hubiera alterado ningún permiso.
	A.6.1.5 Seguridad de la información en la Gestión de proyectos.	Defina procedimientos que establezca la participación del grupo de seguridad en la evaluación y cumplimiento de la protección de la información y lineamientos corporativos.
	A.6.1.1 Roles y responsabilidades para la seguridad de la información.	Configure los sistemas para que generen una entrada de registro y una alerta cuando se agregue o elimine una cuenta a cualquier grupo que tenga asignados privilegios administrativos: * Configure los sistemas para generar una entrada de registro y una alerta de inicios de sesión fallidos en una cuenta administrativa. * Regularmente, revise los registros para identificar anomalías o eventos anormales.
R03-R08-R13-R18-R23-R28 R33-R38-R43-R48-R53-R58 R63-R68-R73-R78-R83-R88 R93-R98-R103-R108-R113 R118-R123-R128-R133-R138 R143-R148-R153-R158-R163 R168-R173-R178-R183-R188 R193-R198-R203-R208-R213 R218-R223-R228-R233-R238 R243-R248-R253-R258	A.12.1.1 Documentación de procedimientos de operación.	Todo cambio desarrollado se debe controlar y documentar de acuerdo con las decisiones o aceptaciones que se presentaron en el comité de cambios.
	A.17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	La compañía debe garantizar la redundancia de los sistemas de información, no solo desde los componentes propios de los sistemas, sino también desde el punto de vista arquitectura. Y estos planes de mitigación deben ser puestos a prueba a fin de garantizar su correcto desempeño y tiempos de respuesta al momento de requerirse.
	A.13.1.2 Seguridad de los servicios de red.	Se debe implementar canales de transmisión redundantes, lo cual implica que los equipos de comunicación y definición de protocolos siempre se encuentren activos para no generar una indisponibilidad.
	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones.	Implemente herramientas de actualización de software automatizadas para garantizar que el software de terceros en todos los sistemas esté ejecutando las actualizaciones de seguridad más recientes proporcionadas por el proveedor de software.
	A.9.2 Gestión de los derechos de acceso asignados a usuarios.	Los administradores de la plataforma deberán tener un compromiso de revisar periódicamente los derechos de acceso de los usuarios, para validar que no se hubiera alterado ningún permiso.

Riesgo	Control de la Norma	Estrategia
R04-R09-R14-R19-R24-R29 R34-R39-R44-R49-R54-R59 R64-R69-R74-R79-R84-R89 R94-R99-R104-R109-R114 R119-R124-R129-R134-R139 R144-R149-R154-R159-R164 R169-R174-R179-R184-R189 R194-R199-R204-R209-R214 R219-R224-R229-R234-R239 R244-R249-R254-R259	A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información. A.11.1.3. Seguridad de oficinas, recintos e instalaciones.	Establecer controles para informar las responsabilidades y deberes en la seguridad de la información, además de concientizar y capacitar al personal en materia de seguridad de la información de acuerdo con sus roles en las áreas de trabajo. La organización establecerá medidas disciplinarias para saber cómo actuar en caso de que se cometa alguna violación de seguridad. Identifique las áreas u oficinas sensibles y establezca controles de acceso biométricos o mediante tarjetas.
	A.7.1.1 Investigación de antecedentes.	Defina procedimientos que establezca el cumplimiento en la consulta de antecedentes disciplinarios para el personal contratado.
	A.8.1.3. Uso aceptable de los activos.	Establecer controles para informar las responsabilidades y deberes en la seguridad de la información, además de concientizar y capacitar al personal en materia de seguridad de la información de acuerdo con sus roles en las áreas de trabajo. La organización establecerá medidas disciplinarias para saber cómo actuar en caso de que se cometa alguna violación de seguridad.
	A.12.1.1 Documentación de procedimientos de operación.	Todo cambio desarrollado se debe controlar y documentar de acuerdo con las decisiones o aceptaciones que se presentaron en el comité de cambios.
	A.13.2.4. Acuerdos de confidencialidad o no divulgación.	Mantener un inventario de información confidencial: Mantener un inventario de toda la información confidencial almacenada, procesada o transmitida por los sistemas de tecnología de la organización, incluidos los que se encuentran en el sitio o en un proveedor de servicios remoto.
	A.6.1.1 Roles y responsabilidades para la seguridad de la información.	Configure los sistemas para que generen una entrada de registro y una alerta cuando se agregue o elimine una cuenta a cualquier grupo que tenga asignados privilegios administrativos: * Configure los sistemas para generar una entrada de registro y una alerta de inicios de sesión fallidos en una cuenta administrativa. * Regularmente, revise los registros para identificar anomalías o eventos anormales.
R05-R10-R15-R20-R25-R30 R35-R40-R45-R50-R55-R60 R65-R70-R75-R80-R85-R90 R95-R100-R105-R110-R115 R120-R125-R130-R135-R140	A.6.1.1 Roles y responsabilidades para la seguridad de la información.	Configure los sistemas para que generen una entrada de registro y una alerta cuando se agregue o elimine una cuenta a cualquier grupo que tenga asignados privilegios administrativos: * Configure los sistemas para generar una entrada de registro y una alerta de inicios de sesión fallidos en una cuenta administrativa. * Regularmente, revise los registros para identificar anomalías o eventos anormales.

Riesgo	Control de la Norma	Estrategia
R145-R150-R155-R160-R165 R170-R175-R180-R185-R190 R195-R200-R205-R210-R215 R220-R225-R230-R235-R240 R245-R250-R255-260	A.12.1.1 Documentación de procedimientos de operación.	Todo cambio desarrollado se debe controlar y documentar de acuerdo con las decisiones o aceptaciones que se presentaron en el comité de cambios.
	A.9.3.1. Uso de información de autenticación secreta.	Se deben implementar una política y unas medidas de seguridad de acceso remoto, para proteger la información a la que se tiene acceso por medio de la conexión de su residencia, que es procesada o almacenada en los lugares en los cuales realiza teletrabajo por medio de factores de autenticación.
	A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información.	Establecer controles para informar las responsabilidades y deberes en la seguridad de la información, además de concientizar y capacitar al personal en materia de seguridad de la información de acuerdo con sus roles en las áreas de trabajo. La organización establecerá medidas disciplinarias para saber cómo actuar en caso de que se cometa alguna violación de seguridad.

Firma: _____

Aprobado por: Wilson Adiel Rodríguez Rodríguez
Jefe Oficina de Tecnologías de la Información y las Comunicaciones OTIC

Elaborado: Julio Andrés Sánchez Sánchez
Contratista OTIC