PLAN DE TRATAMIENTOS DE RIESGOS SEGURIDAD DE LA INFORMACIÓN

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

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE EDUCACIÓN

BOGOTÁ

Enero 2022

Tabla de Contenido

1. JUSTIFICACIÓN 5
2. METODOLOGIA 6
3. OBJETIVO 6
4. ALCANCE 6
5. VALORACION DEL RIESGO 6
   5.1. Valoración de riegos 6
   5.2. Identificación de riesgos inherentes de seguridad digital 7
   5.3. Identificación de Amenazas 7
   5.4. Identificación de Activos de información 8
   5.5. Determinar la criticidad del activo 13
   5.6. Clasificación de activos 14
6. ANALISIS DE RIESGOS 16
   6.1. Definición de niveles de evaluación de impacto 16
   6.2. Determinación de la probabilidad 17
   6.3. Identificación de amenazas por activo 18
   6.4. Evaluación de riesgos 26
   6.5. Mapa de riesgos 26
7. PLAN DE TRATAMIENTO DE RIESGOS 28
   7.1. Aplicación de controles 28

Índice de Tablas

Tabla 1 Definición de amenazas 7
Tabla 2 Activos de información 8
Tabla 3 Criterios de clasificación de activos..... 13
Tabla 4 Valoración de activos 14
Tabla 5 Niveles de impacto 16
Tabla 6 Niveles de probabilidad 17
Tabla 7 Criterios de clasificación de amenazas 18
Tabla 8 Valor del riesgo 19
Tabla 9 Criterios de clasificación de riesgo 26
Tabla 10 Mapa de calor general..... 27
Tabla 11 Opciones tratamiento de riesgo..... 28
Tabla 12 Definición de controles 28

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 2021, 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, 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.

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 aprobada por la SED mediante el documento GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES con fecha de resolución 2-10/Nov/2020, la cual se basa en el 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.".

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 RedP 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 OAREDP 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:

---

2 http://sig.redp.edu.co/Isolucion/Administracion/frmFrameSet.aspx?Ruta=Li4vRnJhbWVTZXRBcnRpY3Vsby5hc3A/UGFnaW5hPUJhbmNvQ29ub2NpbWllbnRvNFNFRFByby8xLzExYjk1NmJiMmI4NjRkMjRiOTA3ZGNlNDIyNTA5NWFmLzExYjk1NmJiMmI4NjRkMjRiOTA3ZGNlNDIyNTA5NWFmLmFzcCZJREFSVElDVUxPPTUwNDU=

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.

-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

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

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.
AI01	Ataque informático	De acuerdo a la tendencia cambiante en las tecnologías de información como informáticas, se hace necesario estar a la vanguardia de los nuevos desafíos 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 el proceso de Gestión de Tecnologías de Información y Comunicaciones, sea tomado el inventario de sistemas de información de la entidad, que se detallan en el cuadro activos de información.

Tabla 2 Activos de información

ID	Nombre Activo	Descripción	Tipo
S001	Construcciones	Herramienta para consolidar y hacer seguimiento a los proyectos de construcción y adecuaciones de los establecimientos educativos. Está compuesta por los siguientes módulos: *Gestión del suelo *Mejoramientos *Proyectos de Infraestructura	Software
S002	Alertas	Permite a los colegios del Distrito reportar y realizar seguimiento a los eventos o situaciones de presunta vulneración de los derechos de las niñas, niños y jóvenes que se presentan en el interior de los colegios o fuera de estos.	Software
S003	Sistema de Inventarios SAE SAI - NVC	Permite la administración del inventario que posee la Secretaría de Educación del Distrito en sus tres niveles, Central, Local y Colegios (recursos SED), tanto de elementos devolutivos como elementos de consumo.	Software
S004	Sistema de Apoyo Escolar	Sistema de Información que permite a los colegios optimizar la gestión operativa que se desarrolla alrededor de los procesos académicos de los estudiantes y que les da la posibilidad de ser autónomos en la generación e impresión de los reportes académicos.	Software
S005	IFindIt	Aplicativo de Búsqueda Empresarial. Usos: tablero de control, Buscador de archivos y portales WEB Las herramientas que hacen parte del aplicativo son: 1. Banco de Preguntas - Despacho 2. Carga Masiva y OCR - Gestión Documental 3. Control Asuntos Políticos - Despacho 4. Buscador Gestión Documental - DSA (Gestión Documental) 5. Buscador Conceptos FSE - Dirección de Contratos 6. Buscador Portal Web (Buscador General y Normatividad)	Software
S006	Sistema Seguimiento a Egresados	Sistema de información para monitorear y analizar las trayectorias de los estudiantes egresados en la educación media oficial de Bogotá, con énfasis en los estudiantes de proyectos media, Sena articulación y los beneficiarios de los fondos para el acceso a la educación superior.	Software
S007	Gestión de Contratos	Aplicación WEB cuyo fin es, apoyar los procesos internos de la Dirección de Contratación, y además lograr consolidar en un sistema toda la información generada en las diferentes etapas del proceso de contratación.	Software
S008	Suma de Sueños	La Dirección de Inclusión aplica anualmente una encuesta a la población estudiantil de alumnos entre los grados 4 y 11, la cual le permite identificar los estudiantes que se clasifican dentro de trabajo infantil o que están en riesgo	Software
S009	Si me conoces Primera Infancia	Permite realizar la consolidación de la información relacionada con las actividades del proceso de Primera Infancia de la Dirección de Educación Preescolar y Básica de la SED, para llevar a cabo el seguimiento y control de las atenciones prestadas a los niños y niñas en las Instituciones Educativas.	Software

ID	Nombre Activo	Descripción	Tipo
S010	SVDI Sistema Integral de Valoración Infantil	Permite aplicar elementos de valoración a niños de primera infancia, a través de la aplicación de los elementos de valoración de acuerdo con la edad del niño, para la generación y producción de conocimiento en torno al desarrollo de niños y niñas en Bogotá.	Software
S011	Construcciones Project Online	Solución de Project Online con reportes desarrollados en Power BI alojados en el DATA LAKE.	Software
S012	Instituciones	Solución implementada en la SED la cual permite centralizar la información y la interacción entre los módulos implementados en las áreas de la entidad.	Software
S013	Si me conoces - Monitoreo	Permite la recopilación de datos a nivel de Institución Educativa para medir la calidad de la educación inicial con base en estándares definidos para evaluar varios aspectos.	Software
S014	PS Documents	Sistema de información permite controlar el inventario de los expedientes físicos que están en custodia del Archivo Central de la SED, adicionalmente apoya el control de préstamos de dichos expedientes.	Software
S015	Servicios públicos	Permite la administración y control sobre el pago de las facturas de los Servicios Públicos generados en los colegios y sedes administrativas de la SED.	Software
S016	Si me conoces - Jornada Única	Permite la administración de los tipos de actividad pedagógica complementarias, estrategias de actividades, modalidades para extensión de jornada educativa, entidades aliadas, ambientes de aprendizaje, líneas pedagógicas, áreas obligatorias reconocidas por la ley 115 y configuraciones de proyectos pedagógicos de Jornada única.	Software
S017	Arrendamientos	Permite la gestión sobre el pago del canon mensual de los predios que la SED toma en arriendo a través de un contrato de arrendamiento.	Software
S018	Humano	El Sistema Humano es una base tecnológica que soporta integralmente los procesos y procedimientos de la gestión del Talento Humano.	Software
S019	Gestión de Cobertura - APEX	Permite el registro de solicitud de inscripciones y traslados por parte de los padres de familia.	Software
S020	Apoteosys	El Sistema de Información Financiero cuenta con una solución modular para soportar la gestión de la entidad, a través de un manejo eficiente e integrado de la información, que se genera en los procesos financieros, donde se hace el seguimiento, ejecución y control del presupuesto de la entidad y los pagos de los proveedores y contratistas.	Software
S021	Matriz CHIP (Contable)	Permite a los Fondos de Servicios Educativos (FSE) de los colegios del Distrito reportar la información de los balances contables.	Software
S022	SI CAPITAL FSE	Sistema de información que integra el proceso financiero, administrativo y de inventarios en los Fondos de Servicios Educativos (FSE), está conformado por los módulos: Predis, Pac, Opget, Sico, Sae, Sai, Limay, Usr-Administración de Usuarios y Sit-Terceros.	Software

ID	Nombre Activo	Descripción	Tipo
S023	Movilidad Escolar	Permite la inscripción y asignación de rutas escolares o subsidio de transporte a los estudiantes de los colegios distritales.	Software
S024	Evaluación Docente	Permite la evaluación del desempeño y del periodo de Prueba para los docentes y directivos docentes en propiedad, cumpliendo con el decreto 1278 del 2002.	Software
S025	SIARA Sistema de Investigaciones Administrativas y Recursos de Apelación	Seguimiento y control de los expedientes relacionados con Investigaciones Administrativas.	Software
S026	Recobro de incapacidades docentes	Registro, administración, seguimiento y control sobre las liquidaciones de incapacidad de los docentes y su recobro a la Fiduprevisora.	Software
S027	POA Plan Operativo Anual	Modulo POA Institucional	Software
S028	SAETA	Aplicativo para seguridad y administración de usuarios.	Software
S029	DUEB Directorio Único de Establecimientos Educativos de Bogotá	Sistema para la gestión de los datos de los establecimientos educativos de Bogotá.	Software
S030	Dexon	Sistema de Información de Mesa de Servicios el cual permite el registro y gestión de las solicitudes realizadas por los funcionarios de los tres niveles institucionales a la mesa de servicios de Redp y la Dirección de Servicios Administrativos.	Software
S031	SIAI Sistema Integrado de Acceso e Ingreso	Permite controlar el acceso a los sistemas que hacen parte de los componentes de extensión de CRM.	Software
S032	Documentos Seguros	Permite gestionar el flujo de trabajo de los documentos relacionados con actos administrativos que emite la SED hasta su formalización e impresión, brindando a los documentos seguridad interna y externa a través de certificados digitales y código de barras, Parametrización y categorización de los documentos, cargue de documentos y ejecución de flujos de revisión y aprobación creación de listas masivas para firmado digital creación de listas masivas de Impresión (creación de PDF).	Software
S033	Escalafón	Contiene el consolidado de títulos reportados por las universidades e incluye el histórico de novedades (inscripciones y ascensos) de docentes privados.	Software
S034	Tiempo de Servicios Docentes Privados	Permite consolidar la información del tiempo de servicio laborado por los docentes en instituciones privadas.	Software
S035	KOMBO	Sistema de Información para la gestión de Nómina.	Software
S036	Audiencia Docente	Aplicación para seleccionar las vacantes ofertadas para los funcionarios que entrega la CNSC dentro de una lista de elegibles a través de audiencias públicas de selección.	Software

ID	Nombre Activo	Descripción	Tipo
S037	Traslados docentes	Herramienta que permite el registro de solicitudes de traslado educadores del Distrito, traslados educadores de los otros entes, permutas de docentes del Distrito y asignación automática de las plazas vacantes de acuerdo con criterios definidos por el Ministerio de Educación y la SED.	Software
S038	Planta	Herramienta Access que permite el registro de novedades de Personal, expedición de actos administrativos, identificación de vacantes en la planta y registro de las diferentes novedades de personal.	Software
S039	Certificados Historia Laboral	Plantilla Access para elaboración de certificados de docentes, para tiempos de servicio e historial laboral	Software
S040	IMAG Información del Magisterio de la SED	Aplicativo de control y trazabilidad de los trámites de prestaciones sociales de docentes y directivos de la Secretaría de Educación Distrital.	Software
S041	Reubicaciones administrativas	Permite el registro de solicitudes de traslado o reubicación de funcionarios administrativos.	Software
S042	Selección de docentes provisionales	Permite apoyar el cubrimiento provisional de vacantes temporales o definitivas sobre la planta docente de la SED.	Software
S043	INFOMAG Fondo Prestacional del Magisterio	Permite realizar el registro y seguimiento a cada una de las solicitudes de prestaciones sociales que efectúan los docentes. Registro de la solicitud de prestación social de un docente, registro de actuaciones realizadas sobre el trámite de solicitud control de estados de solicitud.	Software
S044	Encargos Directivos Docentes	Permite apoyar el proceso de postulación y selección de los docentes que aspiran a cargos de directivos docentes, mediante encargo.	Software
S045	Servicio al ciudadano	Centraliza todas las atenciones o solicitudes que son realizadas por las instituciones educativas, docentes, estudiantes o acudientes a la Secretaría Distrital de Educación.	Software
S046	Fondo de Ahorro y Vivienda Distrital	Aplicativo para la expedición de certificaciones y estado de afiliación de docentes a FAVIDI.	Software
S047	Matriz CHIP (Presupuestal)	Permite que los Colegios del Distrito (FSE) reporten la información del proyecto de presupuesto anual y su ejecución presupuestal.	Software
S048	SIGA	Sistema de información que permite gestionar la correspondencia en los tres niveles de atención de la SED (Nivel central, Direcciones locales y colegios).	Software
S049	Digiturno	Herramienta de apoyo que permite gestionar las necesidades de interacción con los usuarios de la SED en los diferentes puntos de atención.	Software

ID	Nombre Activo	Descripción	Tipo
S050	FUT - Formulario Único de Trámites	Aplicativo web para el registro de trámites referentes a temas educativos que ofrece la entidad.	Software
S051	Consulta Diplomas	Aplicativo para consulta de diplomas de estudiantes.	Software
S052	Isolucion	Sistema de Gestión de Calidad, Abarca todas las áreas de la entidad, incluyendo su direccionamiento estratégico, la planeación de la calidad, sus procesos y procedimientos y el control documental que de estos se deriva.	Software

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 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.

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.

Tabla 4 Valoración de activos

ID Activo	Valoración		
	Conf.	Int.	Disp.
S001	3	2	2
S002	1	1	2
S003	2	3	3
S004	1	1	2
S005	1	2	1
S006	1	2	1
S007	2	1	1
S008	1	2	1
S009	1	2	1
S010	1	2	1
S011	1	2	1
S012	1	1	2
S013	2	2	2
S014	1	1	1
S015	2	1	1
S016	1	1	1
S017	3	3	3
S018	2	1	2
S019	3	2	3
S020	2	2	2
S021	3	2	2
S022	2	2	3
S023	3	2	1
S024	3	2	1
S025	2	1	1
S026	1	2	1
S027	3	2	3
S028	1	1	2
S029	1	2	1

ID Activo	Valoración		
	Conf.	Int.	Disp.
S030	3	2	3
S031	2	3	2
S032	2	2	1
S033	2	2	1
S034	3	3	3
S035	1	2	1
S036	2	1	1
S037	2	3	1
S038	2	2	1
S039	2	1	1
S040	1	1	1
S041	1	2	2
S042	2	2	1
S043	2	1	2
S044	2	3	3
S045	1	2	2
S046	1	2	2
S047	2	2	3
S048	1	1	3
S049	1	1	3
S050	1	2	1
S051	2	2	2
S052	1	1	3

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.

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.
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.
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.

Niveles de Clasificación	Impacto (consecuencias) Cualitativo
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
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

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
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
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

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
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
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

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
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
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

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
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
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

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
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
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

Activo	Amenaza	Impacto	Probabilidad	Riesgo Inherente	ID Riesgo
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
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

Probabilidad	Casi Seguro					
	Probable					
	Posible	R01-R06-R21-R78 R133-R178-R183 R188-R193-R198 R128-R163-R203 R208-R213-R218 R168-R228-R254 R23-R26-R38-R43 R48-R53-R63-R73	R04-R05-R07-R99 R08-R58-R86-R68 R11-R12-R13-R259 R83-R93-R103 R118-R123-R143 R158-R234-R244 R249	R18-R33-R87-R31 R88-R89-R97-R16 R98-R100-R107 R108-R110-R112 R113-R115-R137 R138-R140-R148 R152-R153-R155 R172-R173-R175 R223-R239		
	Improbable	R61-R71-R79-R80 R22-R24-R126 R134-R102-R25 R135-R130-R226 R157-R161-R169 R170-R129-R75 R131-R179-R180 R181-R184-R164 R165-R185-R186 R189-R190-R166 R176-R191-R194 R195-R196-R199 R200-R201-R204 R205-R206-R209 R210-R211-R214 R215-R216-R219 R220-R229-R230 R251-R252-R255 R28-R29-R30-R36 R39-R40-R41-R44 R45-R46-R49-R50 R51-R54-R55-R64 R65-R74-R76	R03-R09-R10-R260 R14-R15-R56-R247 R59-R101-R241 R60-R66-R69-R121 R81-R84-R85-R91 R94-R95-R104 R116-R119-R120 R124-R125-R141 R144-R70-R160 R145-R156-R159 R231-R232-R235 R242-R245-R246 R250-R256-R257 R105	R17-R20-R34-R114 R35-R90-R96-R149 R106-R109-R111 R136-R139-R146 R150-R151-R154 R174-R221-R224 R236-R237-R240 R171-R225		
	Raro	R27-R37-R42-R47 R52-R62-R72-R77 R127-R132-R162 R167-R177-R182- R187-R207-R253 R192-R197-R202- R212-R217-R227-	R67-R57-R142 R82-R92-R117 R233-R243-R122 R248-R258-R02	R19 R32 R147 R222 R238		
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		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 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; 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-	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.

Riesgo	Control de la Norma	Estrategia
R181-R186 R191-R196-R201-R206-R211 R216-R221-R226-R231-R241 R246-R251-R256	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 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.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.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-	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.

Riesgo	Control de la Norma	Estrategia
R183-R188 R193-R198-R203-R208-R213 R218-R223-R228-R233-R238 R243-R248-R253-R258	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.
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.

Riesgo	Control de la Norma	Estrategia
	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 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.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.
	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 Administrativa REDP

Elaborado: Juan Carlos Parra Moreno

Profesional Contratista Oficina Administrativa de REDP