CUERPO OFICIAL DE
BOMBEROS
DOSQUEBRADAS

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BOMBEROS DOSQUEBRADAS

2026

1. INTRODUCCIÓN

En un mundo cada vez más interconectado y digital, la gestión segura de la información se ha convertido en un imperativo fundamental para todas las organizaciones, incluido el Cuerpo Oficial de Bomberos de Dosquebradas. Reconociendo la importancia crítica de salvaguardar la confidencialidad, integridad y disponibilidad de la información sensible y estratégica, nuestra Institución se embarca en la creación de un Plan de Tratamiento y Seguridad de la Información.

Este plan representa un hito significativo en nuestra búsqueda constante de la excelencia operativa y la protección de los intereses de quienes servimos. La transformación digital, si bien trae consigo numerosos beneficios y eficiencias, también conlleva riesgos inherentes que debemos abordar de manera proactiva y estratégica.

En esta introducción, delinearemos los objetivos fundamentales de nuestro Plan de Tratamiento y Seguridad de la Información, destacando la importancia de proteger los activos de información crítica, cumplir con las regulaciones vigentes y, en última instancia, garantizar la confianza de nuestra comunidad y partes interesadas.

A lo largo de este documento, exploraremos las políticas, procedimientos y medidas de seguridad que implementaremos para salvaguardar la información confidencial, al tiempo que promoveremos una cultura de conciencia y responsabilidad en todos los niveles de nuestra organización.

Este plan es una declaración de nuestro compromiso con la seguridad de la información y representa un esfuerzo conjunto para garantizar que los datos que manejamos estén protegidos contra amenazas cibernéticas, accesos no autorizados y posibles interrupciones en nuestras operaciones.

A medida que avanzamos en la implementación de este Plan de Tratamiento y Seguridad de la Información, esperamos fortalecer nuestra capacidad para enfrentar los desafíos del entorno digital actual y, al mismo tiempo, ofrecer un servicio de bomberos eficiente y seguro a nuestra comunidad.

Para la vigencia 2026, el presente Plan de Tratamiento de Riesgos se actualiza teniendo en cuenta la revisión del contexto tecnológico institucional, los avances en la digitalización de procesos, la adopción gradual de servicios bajo el enfoque Cloud First y la evaluación del uso de herramientas de inteligencia artificial como apoyo a la gestión administrativa, en concordancia con el Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETIC vigente.

2. OBJETIVO

Se busca implementar los mecanismos para la gestión de riesgos de Seguridad y Privacidad de la información con el fin de preservar la privacidad, seguridad, integridad y disponibilidad de la información y desarrollar de manera adecuada los procesos misionales, estratégicos y administrativos del Cuerpo Oficial de Bomberos de Dosquebradas.

3. OBJETIVOS ESPECÍFICOS

- ✓ Implementar un sistema de gestión de seguridad de la información (SGSI) basado en las normativas vigentes, incluyendo la Ley 1581 de 2012 y el Decreto 1074 de 2015, para garantizar el cumplimiento de las obligaciones legales en materia de protección de datos personales.

- ✓ Identificar y catalogar todos los activos de información crítica y los datos personales que maneja la institución, incluyendo sistemas, documentos, registros y bases de datos.

- ✓ Realizar una evaluación de riesgos de seguridad de la información de manera periódica para identificar las amenazas potenciales, evaluar la probabilidad e impacto de los riesgos y priorizar la implementación de controles de seguridad.

- ✓ Establecer políticas y procedimientos de seguridad de la información que definan claramente las responsabilidades, prácticas recomendadas y requisitos de cumplimiento para todos los empleados y partes interesadas.

- ✓ Implementar controles de acceso adecuados para garantizar que solo las personas autorizadas tengan acceso a la información confidencial y crítica.

- ✓ Desarrollar programas de concientización y formación en seguridad de la información para educar a los empleados y fomentar una cultura de seguridad en toda la organización.

- ✓ Establecer protocolos para la detección, reporte y respuesta a incidentes de seguridad de la información, con el objetivo de minimizar el impacto de cualquier brecha de seguridad.

- ✓ Garantizar el cumplimiento de las regulaciones y normativas relevantes en materia de seguridad de la información, incluyendo aquellas aplicables a la gestión de datos personales.

- ✓ Incorporar acciones de tratamiento de riesgos asociadas al uso de servicios en la nube, herramientas de inteligencia artificial y software institucional, garantizando la seguridad y privacidad de la información.

- ✓ Establecer procesos para la revisión y mejora continua de las medidas de seguridad de la información, adaptándolas a las cambiantes amenazas y necesidades de la organización.

4. MARCO NORMATIVO

Ley 1581 de 2012 - Protección de Datos Personales: Esta ley regula la protección de datos personales en Colombia. Establece los principios y requisitos para el manejo de datos personales, incluyendo la obtención de consentimiento, la seguridad de los datos y los derechos de los titulares de datos. También establece la Superintendencia de Industria y Comercio como la autoridad de control en temas de protección de datos.

Decreto 1074 de 2015 - Reglamentario de la Ley 1581 de 2012: Este decreto reglamenta la Ley 1581 y proporciona detalles adicionales sobre cómo las organizaciones deben cumplir con las disposiciones de protección de datos personales.

Ley 1273 de 2009 - Delitos Informáticos: Esta ley establece los delitos informáticos en Colombia y las penas asociadas a ellos. Incluye disposiciones relacionadas con el acceso no autorizado a sistemas y datos, así como la interceptación ilegal de comunicaciones.

Ley 527 de 1999 - Firma Electrónica: Esta ley regula el uso de firmas electrónicas y mensajes de datos en Colombia. Establece la validez legal de las transacciones electrónicas y la firma electrónica como un medio de autenticación.

Decreto 620 de 2005 - Política de Seguridad de la Información: Este decreto establece la política de seguridad de la información para las entidades públicas en Colombia. Establece los lineamientos y requisitos para proteger la información en el sector público.

Norma Técnica Colombiana NTC-ISO/IEC 27001: Esta norma es la versión colombiana de la norma internacional ISO/IEC 27001, que establece los requisitos para un sistema de gestión de seguridad de la información. Es utilizada por organizaciones para implementar controles de seguridad de la información.

Decreto 1377 de 2013 - Registro Nacional de Bases de Datos: Este decreto reglamenta el Registro Nacional de Bases de Datos ante la Superintendencia de Industria y Comercio, como parte de las obligaciones establecidas en la Ley 1581.

Circular Externa 002 de 2015 - Superintendencia Financiera de Colombia: Esta circular establece los requisitos de seguridad de la información para las entidades financieras bajo supervisión de la Superintendencia Financiera.

5. ALCANCE

Alcance del Plan de Tratamiento y Seguridad de la Información del COBD

El alcance de este Plan de Tratamiento y Seguridad de la Información del Cuerpo Oficial de Bomberos de Dosquebradas (COBD) abarca todas las actividades, recursos y procesos relacionados con la gestión de la información y la seguridad de los datos en la organización. Su objetivo principal es establecer las directrices y los controles necesarios para proteger la confidencialidad, integridad y disponibilidad de la información crítica, garantizando así la continuidad de las operaciones y la satisfacción de las necesidades de las partes interesadas.

El alcance del plan incluye, pero no se limita a, los siguientes aspectos:

- **Identificación de Activos de Información**: Se llevará a cabo un inventario exhaustivo de todos los activos de información, incluyendo datos, sistemas, documentos, registros y cualquier otra forma de información utilizada o generada por el COBD.

- **Evaluación de Riesgos**: Se realizará una evaluación de riesgos para identificar las amenazas potenciales a la seguridad de la información y las vulnerabilidades asociadas a los activos identificados. Esto permitirá priorizar y abordar los riesgos de manera efectiva.

- **Políticas y Procedimientos de Seguridad**: Se establecerán políticas y procedimientos de seguridad de la información que definan las responsabilidades, las prácticas recomendadas y los requisitos de cumplimiento para todos los empleados y partes interesadas.

- **Controles de Acceso**: Se implementarán controles de acceso adecuados para garantizar que solo las personas autorizadas tengan acceso a la información confidencial y crítica.

- **Gestión de Incidentes de Seguridad**: Se establecerán protocolos para la detección, reporte y respuesta a incidentes de seguridad de la información, con el objetivo de minimizar el impacto de cualquier brecha de seguridad.

- **Concientización y Formación**: Se llevarán a cabo programas de concientización y formación en seguridad de la información para educar a los empleados y crear una cultura de seguridad.

- **Cumplimiento Normativo**: Se hará todo lo posible porque el COBD cumpla con las regulaciones y normativas relevantes en materia de seguridad de la información, incluyendo aquellas aplicables a la gestión de datos personales.

- **Evaluación y Mejora Continua**: Se establecerán procesos para la revisión y mejora continua de las medidas de seguridad de la información, adaptándolas a las cambiantes amenazas y necesidades de la organización.

Este plan tiene como objetivo principal asegurar que la información crítica del COBD esté protegida contra amenazas internas y externas, promoviendo así la confianza de las partes interesadas y la efectividad en la prestación de servicios de bomberos en Dosquebradas.

6. RESPONSABLE

La Oficina de Tecnología es la dependencia encargada de la estructuración e implementación del plan de gestión de riesgos de la información.

7. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: Repositorio de información de la cual la entidad realiza algún tipo de tratamiento.

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Ciberseguridad: Capacidad de la Institución para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las

actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Probabilidad: es la posibilidad de que algo pueda suceder. La probabilidad puede ser definida, determinada y medida objetiva o subjetivamente, y puede expresarse de forma cualitativa o cuantitativa.

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

8. CONTEXTO

El Cuerpo Oficial de Bomberos de Dosquebradas (COBD) es una entidad dedicada a salvaguardar la vida y los bienes de los ciudadanos en situaciones de emergencia y desastres en el municipio de Dosquebradas. La naturaleza crítica de nuestras operaciones exige la gestión segura de la información y datos, ya que esta información desempeña un papel esencial en la toma de decisiones, la planificación de respuestas efectivas y la coordinación de esfuerzos en situaciones de crisis.

El COBD, en su constante búsqueda de la excelencia en el servicio y la adaptación a los desafíos modernos, ha iniciado un proceso de Transformación Digital para mejorar la eficiencia y la capacidad de respuesta en sus operaciones. Este proceso implica una mayor dependencia de los sistemas de información y tecnología, lo que a su vez aumenta la importancia de salvaguardar la seguridad y privacidad de la información digital y física.

La creación del presente documento de Seguridad y Privacidad de la Información es una respuesta a esta necesidad crítica. Este documento se establece como el marco rector que define las políticas, procedimientos y medidas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información crítica del COBD. Además, busca garantizar el cumplimiento de las regulaciones vigentes relacionadas

con la seguridad de la información, incluyendo aquellas que afectan a la gestión de datos personales y la transparencia en el Gobierno Digital.

La seguridad y privacidad de la información no son solo un imperativo legal y operativo, sino también un compromiso ético con la comunidad a la que servimos. Este documento se basa en principios fundamentales de responsabilidad, integridad y transparencia, que son inherentes a la misión del COBD.

En un entorno de crecientes amenazas cibernéticas y desafíos de seguridad, la protección de la información es esencial para preservar la confianza de nuestra comunidad y garantizar una respuesta eficiente en momentos de crisis. Este documento representa el compromiso del COBD de ser un líder en seguridad de la información en el ámbito de los servicios de emergencia y una garantía de que nuestros ciudadanos pueden confiar en nosotros en los momentos en que más nos necesitan.

Este contexto establece las bases para la creación de un sólido marco de seguridad y privacidad de la información que fortalecerá nuestras operaciones y contribuirá a nuestra misión de salvar vidas y proteger bienes en Dosquebradas. En las siguientes secciones de este documento, se detallarán las políticas, procedimientos y medidas específicas que garantizarán la seguridad y privacidad de la información en toda la organización del COBD.

8.1. CONTEXTO TECNOLÓGICO 2026

Para la vigencia 2026, el contexto tecnológico del El Cuerpo Oficial de Bomberos de Dosquebradas (COBD) contempla una mayor dependencia de los sistemas de información para la gestión administrativa y operativa, así como la adopción progresiva de servicios en la nube y herramientas tecnológicas de apoyo.

Adicionalmente, se identifica el uso potencial de herramientas de inteligencia artificial para actividades de análisis, automatización y apoyo administrativo, lo cual amplía la superficie de riesgo y hace necesario fortalecer los controles de seguridad y privacidad de la información.

9. IDENTIFICACIÓN DE AMENAZAS

- ✓ ***Ataques Cibernéticos***: Esto incluye ataques de malware, ransomware, virus, troyanos y ataques de denegación de servicio (DDoS) que pueden interrumpir los sistemas y robar o bloquear el acceso a la información crítica.

- ✓ ***Phishing y Ingeniería Social***: Los ataques de phishing buscan engañar a los empleados para que divulguen información confidencial, como contraseñas, a través de correos electrónicos o mensajes falsos. La ingeniería social involucra la manipulación psicológica para obtener información confidencial.

- ✓ ***Fuga de Datos***: La pérdida o filtración de información sensible debido a errores humanos, brechas de seguridad o empleados deshonestos.

- ✓ ***Acceso No Autorizado****:* La falta de control de acceso adecuado puede permitir que personas no autorizadas accedan a sistemas o información confidencial.

- ✓ ***Vulnerabilidades de Software***: Las vulnerabilidades en software y sistemas operativos pueden ser explotadas por atacantes para obtener acceso no autorizado.

- ✓ ***Dispositivos No Gestionados***: Dispositivos personales no gestionados, como teléfonos móviles y tabletas, pueden representar riesgos de seguridad si se conectan a la red corporativa.

- ✓ ***Acceso Físico no Autorizado***: La falta de seguridad física en las instalaciones podría permitir a personas no autorizadas acceder a servidores u otros recursos críticos.

- ✓ ***Desastres Naturales y Daños Físicos***: Incendios, inundaciones y otros desastres naturales pueden dañar equipos y sistemas críticos.

- ✓ ***Fallas de Energía y Equipamiento***: Interrupciones de energía eléctrica y fallas de equipos pueden causar pérdida de datos y tiempo de inactividad.

- ✓ ***Cumplimiento Normativo Inadecuado***: No cumplir con las regulaciones de seguridad de la información puede resultar en sanciones legales y pérdida de confianza.

- ✓ ***Amenazas Internas***: Acciones maliciosas o descuidadas por parte de empleados pueden representar un riesgo para la seguridad de la información.

- ✓ ***Interconexión de Sistemas***: La interconexión de sistemas con terceros puede exponer a la organización a vulnerabilidades externas.

- ✓ ***Actualizaciones y Parches no Aplicados***: No aplicar actualizaciones de seguridad y parches puede dejar sistemas vulnerables a amenazas conocidas.

- ✓ ***Proveedores de Servicios***: Los proveedores de servicios pueden ser un vector de amenaza si no tienen prácticas de seguridad sólidas.

- ✓ ***Escasez de Recursos***: La falta de recursos, tanto financieros como de personal, puede afectar negativamente la capacidad de implementar medidas de seguridad.

- ✓ ***Servicios en la nube***: Configuración inadecuada de servicios en la nube que genere pérdida, acceso no autorizado o indisponibilidad de la información.

- ✓ ***Herramientas de inteligencia artificial***: Uso inadecuado de estas herramientas que implique exposición de información sensible o datos personales.

10. IDENTIFICACIÓN DE VULNERABILIDADES

Las vulnerabilidades básicamente son las debilidades en seguridad y privacidad de la información y se agrupan de la siguiente manera:

- ✓ • Hardware
- ✓ • Red
- ✓ • Software
- ✓ • Persona
- ✓ • Organizacional

- ✓ • Instalaciones
- ✓ • Información

La vulnerabilidad por sí misma no implica la materialización del riesgo la cual podría ser utilizada por una amenaza para su aprovechamiento, la cuales podrían ser las siguientes:

- ✓ ***Software Desactualizado***: No aplicar regularmente actualizaciones y parches de seguridad en sistemas y aplicaciones puede dejarlos vulnerables a explotaciones conocidas.

- ✓ ***Contraseñas Débiles***: El uso de contraseñas débiles o predecibles puede permitir a los atacantes adivinarlas con facilidad y acceder a sistemas o cuentas protegidas.

- ✓ ***Falta de Autenticación de Dos Factores (2FA)****:* La ausencia de autenticación de dos factores aumenta el riesgo de que las cuentas sean comprometidas en caso de que las contraseñas sean robadas.

- ✓ ***Acceso No Controlado*****:** Falta de controles de acceso adecuados que permitan a personas no autorizadas acceder a sistemas o información crítica.

- ✓ ***Malware y Virus***: La falta de una solución de seguridad adecuada puede permitir que el malware y los virus infecten sistemas y redes.

- ✓ ***Falta de Capacitación en Seguridad***: La falta de conciencia y capacitación en seguridad de la información entre los empleados puede dar lugar a errores que comprometan la seguridad.

- ✓ ***Falta de Copias de Seguridad (Backups) Regulares***: No realizar copias de seguridad regulares de los datos puede hacer que la organización sea vulnerable a la pérdida de información en caso de incidentes.

- ✓ ***Dispositivos Desprotegidos****:* No proteger adecuadamente dispositivos como teléfonos móviles y tabletas puede exponer a la organización a riesgos de seguridad.

- ✓ ***Comunicaciones Inseguras***: La falta de cifrado en las comunicaciones puede permitir que los atacantes intercepten y accedan a datos confidenciales.

- ✓ ***Falta de Actualización de Políticas y Procedimientos***: La falta de actualización de políticas y procedimientos de seguridad puede dejar lagunas en la protección de la información.

- ✓ ***Malas Prácticas de Gestión de Contraseñas***: El almacenamiento inseguro de contraseñas o compartirlas sin cuidado puede poner en riesgo la seguridad.

- ✓ ***Redes Inseguras***: Configuraciones de red débiles o inseguras pueden facilitar el acceso no autorizado.

- ✓ ***Acceso Físico no Controlado***: Falta de seguridad física en las instalaciones, como cámaras o acceso restringido, puede permitir el acceso no autorizado a equipos y sistemas.

- ✓ ***Terceros No Seguros***: La falta de debida diligencia en la selección de proveedores y terceros puede exponer a la organización a riesgos.

- ✓ ***Escasez de Personal de Seguridad***: La falta de personal de seguridad de la información dedicado puede llevar a una menor capacidad de identificar y mitigar vulnerabilidades.

11. IDENTIFICACIÓN DE RIESGOS Y CONSECUENCIAS

IDENTIFICACIÓN DE LOS RIESGOS Y CONSECUENCIAS					
ACTIVO	**RIESGO**	**VULNERABILIDAD/ CAUSA**	**AMENAZA**	**DESCRIPCIÓN DEL RIESGO**	**CONSECUENCIAS**
Hardware	Pérdida de la Confidencialidad	Almacenamiento desprotegido	Robo de medios, equipos o documentos.	Posibilidad de divulgación de información de manera no autorizada	Demandas o implicaciones legales por información
	Pérdida de la Disponibilidad			Posibilidad de pérdida de acceso a información que no tiene respaldo	No disponibilidad de información
Hardware	Pérdida de la Integridad	Almacenamiento desprotegido	Manipulación de la información	Modificación de la información	Publicación de información que no es real, responder a la ciudadanía de manera inadecuada

					cu ad a
Hard ware	Pér did a de la Co nfid enc iali da d	Descuid o en la disposic ión final de dispositi vos de almace namient o	Recupe ración de informa ción de medio s recicla dos o descart ados	Que una persona sin autorización de acceso a la información pueda tenerla por falta de cuidado en su disposición.	U so inade cuad o de la inform ación.

Har dw are	Pé rdi da de la Int eg rid ad	Falta de esque mas de reem plazo periód ico	Mal funcio namie nto de dispo sitivos o siste mas	Falta de redundan cias en los equipos y sus compone ntes.	Que la inform ación no se almac ene de mane ra adecu ada y quede desactu alizada
Har dw are	Pér did a de la dis po nib ilid ad da d	Falta de esque mas de reem plazo periód ico. Manten imiento o inadec uado o instala ción	Mal funcio namie nto de dispo sitivos o sistem as	Posibilid ad de falla en los dispositiv os que integran la infraestru ctura de la entidad	Pérdi da de la inform ación o el acces o a ella.

		defectuosa de medios de almacenamiento			
Hardware	Pérdida de la Confidencialidad	Inadecuado control de cambios	Inadecuado control de cambios Pérdida de la disponibilidad	Posibilidad de administración inadecuada de los dispositivos	Riesgo de versiones que permitan acceder a personas
	Pérdida de la Integridad Pérdida de la Disponibilidad			Pérdida de la disponibilidad Que por falla en la administración del equipo no se pueda acceder a los usuarios o al sistema de información.	Que por falla en la administración del equipo no se pueda acceder a los usuarios o al sistema de información. Que por incompatibilidad

					de versiones de software no se pueda acceder a la información.

Hardware	Pérdida de la Disponibilidad	Mantenimiento inadecuado o instalación defectuosa de medios de almacenamiento	Destrucción de dispositivos o medios de almacenamiento	El daño de dispositivos de almacenamiento interno y externo por golpes o fallas del equipo.	Perder la información alojada en el dispositivo de almacenamiento.
	Pérdida de la Integridad		Manipulación de información	No tener políticas claras y fuertes en relación al control de acceso y que pueda ingresar una persona no autorizada.	Alteración de la información institucional sin

Hardware	Pérdida de la Confidencialidad	Sistemas desprotegidos ante acceso no autorizado	Divulgación de información confidencial	No tener políticas claras y fuertes en relación al control de acceso y que pueda ingresar una persona no autorizada.	autorización.
			Acceso no autorizado a sistemas informáticos	No tener herramientas de verificación de acceso	Acceso de personas no autorizadas a información clasificada o reservada
	Pérdida de la Integridad				Alteración de la información institucional sin autorización.
	Pérdida de la Disponibilidad				Eliminación de información por parte de usuarios no orizado

Hardware	Pérdida de la Disponibilidad	Susceptibilidad del equipamiento a alteraciones en el voltaje	Perdida del suministro de energía eléctrica	Alteraciones del flujo de corriente eléctrica con afectación a los equipos de procesamiento de la entidad	Pérdida de información por daño en unidades de almacenamiento
Hardware		Susceptibilidad del equipamiento a la humedad, contaminación, polvo, corrosión o congelamiento	Contaminación, polvo, corrosión o congelamiento	Afectación a los equipos de procesamiento de información, falta de mantenimiento, error en la configuración de la temperatura del centro de datos	Pérdida del acceso a la información por falla en los equipos
Hard	Pérdida de	Susceptibilidad del equipamiento	Fenómenos climáticos y meteorológicos	Afectación a los equipos de procesamiento de información, falla del aire acondicionado por dimensionamiento.	Pérdida de acceso a la informa

ware	la Disponibilidad	a la temperatura	Falla del sistema de aire acondicionado	Afectación a los equipos de procesamiento de información, falta de mantenimiento error o falla en el aire acondicionado del centro de datos.	ción por falla en los equipos
Red	Pérdida de la Confidencialidad	Arquitectura de red insegura	Mala planeación o falta de adaptación	Acceso de personas no autorizadas a los sistemas de información de la entidad.	Mal uso de la información de la entidad.
	Pérdida de la Integridad			Acceso de personas no autorizadas a los sistemas de información de la entidad. Que puedan alterar la información	Alteración de información institucional incluso con consecuencias legales.
	Pérdida de la Disponibili			Acceso de personas no autorizadas a los sistemas de información de la entidad.	Eliminación de información institucional, que pueda llegar a tener

	da d			Que puedan eliminar la informaci ón.	consec uencias legales.
Re d	Pé rdi da de la Co nfi de nci ali da d	Cone xiones de red pública sin protecc ión	Acce so no autori zado a siste mas infor máti cos	Falta de aplicación reglas de administr ación, que brinden segurida d a la red.	Acces o de person as no autoriz adas a inform ación clasific ada o reserv ada.
	Pé rdi da de la Int eg rid ad			Falta de aplicación reglas de administr ación, que brinden segurida d a la red.	Alteraci ones en la informa ción debido al acceso de person as no autoriza das a informa ción clasifica da o reserva da.
	Pé rdi da de la Di sp oni bili da d			Falta de aplicació n de reglas de administr ación, que brinden segurida d a la red.	Elimina ción de informa ción debido al acceso de person as no autoriz adas a informa ción clasific ada o reserva da.

Red	Pérdida de la Confidencialidad	Falta de control en datos de entrada y salida y emisor y receptor	Datos de fuentes no confiables	Acceso a canales de comunicación a personas no autorizadas.	Acceso a información clasificada o reservada a personas no autorizadas
	Pérdida de la Integridad			Acceso a canales de comunicación a personas no autorizadas.	Alteración de información clasificada o reservada por personas no autorizadas
	Pérdida de la Disponibilidad			Acceso a canales de comunicación a personas no autorizadas.	Eliminación de información clasificada o reservada por personas no autorizadas
Red	Pérdida de la Confidencialidad	inadecuada gestión de redes	Error de uso, uso o administración incorrectos de dispo	Acceso no autorizado a los sistemas de información de la entidad por medio del acceso de una red pública.	Divulgación de información reservada y clasificada de la entidad.

	Pérdida de la Disponibilidad		sitivos y sistemas	Acceso no autorizado a los sistemas de información de la entidad.	Eliminación de información.
Red	Pérdida de la Confidencialidad	Malagestión de contraseñas	Robo de identidad	Accesos a sistemas de información a personas no autorizadas	Divulgación de información de manera inadecuada, suplantación
	Pérdida de la Integridad			Accesos a sistemas de información a personas no autorizadas	Divulgación de información de manera inadecuada, suplantación
	Pérdida de la Disponibilidad			Accesos a sistemas de información a personas no autorizadas	Eliminación de información, que puede traer consecuencias legales
Red	Pérdida de la Confidencialidad	Punto único de fallas	Falla de los equipos de Telecomunicaciones	Presentar fallas en equipos de telecomunicaciones centralizados en un punto	Información alterada o

				único y no tener redundancia	desincronizada
	Pérdida de la Integridad				canales de comunicación de la entidad y que afecte su misionalidad.
	Pérdida de la Confidencialidad	Redes accesibles a personas no autorizadas	Robo de identidad	Suplantación de usuario.	Suplantación para uso indebido de la inf

					ormación.
Red	Pérdida de la Disponibilidad	Sobre dependencia en un dispositivo o sistema	Falla de dispositivos o sistemas	Daño del equipo y falta de redundancia de la información	Pérdida total de la información alojada en un solo equipo.
Software	Pérdida de la Confidencialidad	Defectos bien conocidos en el software	Mal funcionamiento to de dispositivos o sistemas	Posibilidad de fallas en el software o sistemas de información, como indisponibilidad, fallas en los cálculos o registro de información o accesos no	Alteraciones en la información, problem
	Pérdida del				

	a Integridad			autorizados debido a los defectos o fallas de los sistemas	aspara el acceso y disponibilidad de la información.
	Pérdida de la Disponibilidad				
Software	Pérdida de la Disponibilidad	Bases de datos con protección desactualizada contra códigos maliciosos	Distribución de software malicioso	Aparición de nuevos códigos maliciosos que afecten los sistemas de información	Eliminación o secuestro de la información de la entidad.
	Pérdida de la Integridad			Aparición de nuevos códigos maliciosos que afecten los sistemas de información	Alteración u ocultamiento de inf

					or maci ón de la en tid ad .

S of t w ar e	Pérdi da de la Confi denci alidad	Contr ase ñas inse gura s	Acce so no autori zado a siste mas infor máti cos	Posibilid ad de acceso no autorizad o a los sistemas de informaci ón y documen tos electróni cos	E x p o s i c i ó n d e i n f o r m a c i ó n c l a s i f i c a d a o r e s e
	Pérdid a de la Integri dad				
	Pérdi da de la Dispo nibili dad				
	Pérdi da de la Confid enci alidad	Defect os bien conoc idos en el softw are	Espio naje por interc eptaci o nes tecnol ógicas		

					rvadadelaentidad
Software	Pérdida de la Confidencialidad	Defectos bien conocidos en el software	Divulgación de información confidencial	Posibilidad del aprovechamiento de vulnerabilidades ampliamente conocidas de los sistemas de información o sistemas operativos usados en la entidad, para obtener información por parte de atacantes	Exposición de información clasificadaadores

					ervadadelaentidad
Software	Pérdida de la Confidencialidad	Descarga y uso no controlado de software	Abuso de derechos o autorizaciones	Descarga de malware o ransomware que realicen intrusión a los sistemas de información	Suplantación de identidad, extracción de inf

					ormación confidencial.
	Pérdida de la Integridad			Descarga de malware o ransomware que realicen intrusión a los sistemas de información	Alteración de los sistemas de información.

	Pérdida de la Disponibilidad			Descarga de malware o ransomware que realicen intrusión a los sistemas de información	Eliminación o secuestro de información.
Software	Pérdida de la Confidencialidad	Descarga y uso incontrolado de software	Distribución de software malicioso	Uso de aplicaciones inseguras que afecten los sistemas de información	Suplantación de identidad, extracción de información confidencial.
	Pérdida de la Integridad				Alteración de los sistemas de informa

					ción
	Pérdida de la Disponibilidad				Eliminación o secuestro de información.
Software	Pérdida de la Confidencialidad	Eliminación de soportes de almacenamiento sin borrado de datos	información de medios reciclados o descartados	Extracción de información de medios de almacenamiento desechados	Acceso a información reservada o clasificada a personal no autorizado.
Softwar	Pérdida de la Disp	Falta de copias de	Destrucción de dispositivos o medios de almacenami	Destrucción no autorizada de información no respaldada.	Pérdida definitiva de información

e	onibilidad	respaldo	ento		de la entidad
			Falla de dispositivos o sistemas	Falla en componentes de sistemas de información.	Pérdida de información por falta de respaldo
Software	Pérdida de la Confidencialidad	Falta de mecanismos de identificación y autenticación	Repudio de acciones	Acceso a sistemas de información de la entidad a personal no autorizado.	Suplantación para gestión de información.
	Pérdida de la Integridad			Alteraciones en los sistemas de información sin verificación de identidad.	Modificaciones en la información sin identificación de

					Usuario real.

Software	Pérdida de la Confidencialidad	Falta de mecanismos de identificación y autenticación	Acceso no autorizado a sistemas informáticos	Suplantación de identidad o acceso a los sistemas de información sin identificación de usuario	Espionaje, acceso a información de carácter clasificado o reservado de la entidad.
	Pérdida de la Integridad				Modificación a la información sin identificación de usuario o con un usuario ajeno.
	Pérdida de la Disponibilidad				Eliminación de información.

Software	Pérdida de la Confidencialidad	Falta de separación de entornos de prueba y operativos	Manipulación de hardware o software	Los programadores o terceros pueden llegar a tener acceso a información a la cual no estuvieran autorizados.	Personas no autorizadas con acceso a la información clasificada o reservada de la entidad.
	Pérdida de la Integridad			Procesar y presentar información de prueba que no esté verificada.	estionar información sin garantías de procesamiento o modificar información de la entidad sin autorización.

	Pérdida de la Disponibilidad			Información eliminada en realización de pruebas.	Eliminación de información de la entidad sin autorización.
Software	Pérdida de la Confidencialidad	nadecuada o falta de implementación de auditoría	Mala planeación o falta de adaptación	Falta de realización de las actividades programadas para la	Falta de verificación de accesos a los sistemas de información.

	Pérdida de la Integridad	interna		implementación de controlesrelacionados con el tratamiento de riesgo en seguridad y privacidad de la información.	Falta de verificación de la calidad de información de la entidad.
	Pérdida de la Disponibilidad				Falta de información en los sistemas de información.
Software	Pérdida de la Confidencialidad	Inadecuado control de cambios	Error de uso, uso o administración incorrectos de dispositivos y siste	Uso de versiones desactualizadas de los sistemas de información, errores de configuración o generación de	Acceso de información a usuarios no autorizados o incog

			mas	permisos.	nitos.
	Pérdida de la Integridad				Cambios en la información o en las condiciones de procesamiento
	Pérdida de la Disponibilidad				
Software	Pérdida de la Confidencialidad	Inadecuados derechos de usuario	Abuso de derechos o autorizaciones	Usuarios administrativos o con altos privilegios que realicen cambios en accesos o configuraciones sin autorización	Brindar acceso a información reservada y clasificada a usuarios no au

					torizados.
	Pérdida de la Integridad				Modificaciones en la información o en sus registros sin autorización.
	Pérdida de la Disponibilidad				Eliminación de información sin autorización ya sea de manera equivocada o premeditada.

Software	Pérdida de la Confidencialidad	Inadecuados derechos de usuario	Divulgación de información confidencial	Posibilidad de exposición de información clasificada o reservada por el acceso de personal no autorizado	Exposición de información clasificada o reservada de la entidad
Software	Pérdida de la Confidencialidad	Incorrecta configuración de parámetros	Mal funcionamiento de dispositivos o sistemas	Error en la configuración de los parámetros de seguridad de los sistemas de información	Procesamiento equivocado de la información.
	Pérdida de la Integridad				Falta de acceso a la información en el momento requerido
	Pérdida de la Disponibilidad				Personas no autorizadas con acceso a los sistemas de infor

					mación.
Software	Pérdida de la Confidencialidad	Interfaz de usuario complicada	Error de uso, uso o administración n incorrectos de dispositivos y sistemas	Falta de conocimiento de los usuarios en el manejo de los sistemas de información	Errores en el tratamiento de la información, de forma involuntaria.
	Pérdida de la Integridad				Borrado de información por falta de manejo de las interfaces.
	Pérdida de la Disponibilidad				Eliminación de información de manera involuntaria.

Software	Pérdida de la Confidencialidad	Malagestión de contraseñas	Robo de identidad	Personas que averigüen el usuario y contraseña de manera inescrupulosa	Uso inadecuado de los sistemas de información
	Pérdida de la Integridad			Eliminación de información de manera intencional por parte de un tercero.	Eliminación de información sin autorización y sin trazabilidad de usuario
	Pérdida de la Disponibilidad			Personas que averigüen el usuario y contraseña de manera inescrupulosa	Uso inadecuado de los sistemas de información
	Pérdida de la	Requi			Procesamiento de la

Software	Confidencialidad	sitos para desarrollo de software no definidos con claridad	Mal funcionamien to de dispositivos o sistemas	Falta de conocimiento de la configuración del software	información erróneo o equivocado
	Pérdida de la Integridad				Borrado de información
	Pérdida de la Disponibilidad				Que existan salidas de información no autorizadas y que pueda llegar a personas no autorizadas.
Software	Pérdida de la Confidenciali	Sesiones activas después del horario	Acceso no autorizado a sistemas	Posibilidad de exposición de información clasificada o reservada	Exposición de información clasi

	dad Pérdida de la Integridad Pérdida de la Disponibilidad	laboral o al dejar la estación de trabajo	informáticos	de manera remota o por atacantes	ficada o reservada de la entidad
Software	Pérdida de la Confidencialidad	Software inmaduro o nuevo	Error de uso, uso o administración incorrectos de dispositivos y	Errores en procesamiento por fallas en la programación y en la configuración del	Procesamiento de información erróneagenerando resultados equivocados.

	Pérdida de la Integridad		sistemas	sistema de información	Borrado de información por error en el procesamiento de información y falta de acceso a los códigos fuente.
	Pérdida de la Disponibilidad				Acceso a terceros no autorizados a los sistemas de información
Soft	Pérdida de la Confide	Software inmaduro	Mal funcionamien to de	Errores en procesamiento por	Procesamiento de información erró

ware	nciali dad	o nuevo	dispo sitivos o sistem as	fallas en el funciona miento de los sistemas de informaci ón	nea gen eran do resu ltad os equiv ocado s.
	Pérdi da de la Integ rid ad				Borr ado de info rma ción por erro r en el proc esa mie nto de infor mació n.
	Pérdi da de la Di spo ni bili da d				Acc eso a terc eros no auto riza dos a los siste mas de infor mac ión

Software	Pérdida de la Confidencialidad	Software no documentado	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Falta de acceso a los códigos fuente de los sistemas, falta de acceso al control de cambios de los sistemas de información, falta de acceso a la documentación de la aplicación que permita la identificación de variables y su	Modificaciones en los procesamientos de información sin identificar su causa
	Pérdida de la Integridad				Borrado de información involuntario o falta de acceso a los sistemas de información a usuarios autorizados

	Pérdida de la Disponibilidad			procesamiento.	Acceso a los sistemas de información a usuarios no autorizados
Software	Pérdida de la Confidencialidad	Tablas de contraseña desprotegidas	Divulgación de información confidencial	Acceso a la información de contraseñas a personas no autorizadas	Personas no autorizadas con acceso a la información que pueden tener y realizar suplantación.
Software	Pérdida de la Integrid	Uso no controlado de sistemas de infor	Manipulación de información	Falta de control de los accesos a los sistemas de	Usuarios no autorizados con

	ad	mación		información	acceso a la información
Persona	Pérdida de la Confidencialidad	Falta o disposiciones insuficientes (relativas a la seguridad) en loscontratos con clientes y / o terceros	Abuso de derechos o autorizaciones	Falta de controles a terceros que realicen tratamiento de información a nombre de la entidad	Información sesgada o mal procesada debido a falta de verificación.
	Pérdida de la Integridad			Falta de acuerdos de nivel de servicio donde se especifique la disponibilidad de los servicios y su soporte	Falta de disponibilidad de los sistemas de información o dificultades para su obtención una vez

					finalizada la relación contractual
	Pérdida de la Disponibilidad			Divulgación de información clasificada o reservada de la entidad	Materialización de riesgo legal en relación al tratamiento de datos personales.
	Pérdida de la Confidencialidad	Acceso no restringido a instalaciones	Robo de medios,equipos o documentos.	Que personas no autorizadas tomen equipos, medios de almacenamiento o documentos	Personas no autorizadas con acceso a información res

					erva da o clasifi cada.
	Pérdida de la Integridad Pérdida de la Disponibilidad				No poder acceder a la información debido a la pérdida del archivo donde se encuentra almacenada.
Persona	Pérdida de la Disponi	Ausencia de personal	Obstaculización de la disponibilidad del perso	Falta de personal con la información o falta de personal para responder a tiempo	Falta de disponibilidad de información a la

	bilidad		nal	requerimientos de información	ciudadanía o entes de control de manera oportuna
Persona	Pérdida de la Confidencialidad	Empleados desmotivados o inconformes	Interceptación de información - Espionaje	Envío de información a terceros no autorizados	Terceros sin autorización con información clasificada o reservada de la entidad.
Persona	Pérdida de la Confidencialidad	Empleados desmotivados o inconformes	Robo de medios, equipos o documentos.	Contratistas o servidores que lleven medios de almacenamiento, equipos o documentos sin autorización.	Personas no autorizadas con acceso a información clasifica

					da y reservada.
	Pérdida de la Disponibilidad				Falta de información por pérdida de equipos o documentos.
	Pérdida de la Disponibilidad	Empleados desmotivados o inconformes	Sabotaje	Sabotajea las condiciones de seguridad a los sistemas de información.	Eliminación o alteración de la información de manera voluntaria y no autorizada por parte de servidor

					es o contratistas.
Persona	Pérdida de la Integridad	Empleados desmotivados o inconformes	Coerción, Extorsión o Corrupción	Alteraciones en la información como informes de gestión.	Cambios en información que puede generar impactos legales.

	Pérdida de la Disponibilidad			Eliminación de información de manera no autorizada.	Eliminación de información sin autorización o falta de acceso a los sistemas de información en momentos necesarios.
	Pérdida de la Confidencialidad			Corrupción conocimiento de información de contratación en condiciones desiguales	Desigualdad en la contratación de proveedores o contratistas.

Persona	Pérdida de la Confidencialidad	Falta de un proceso formal para la revisión del derecho de acceso (supervisión)	Abuso de derechos o autorizaciones	Falta de implementación de un procedimiento de gestión de usuarios	Cambios no autorizados en los sistemas de información con usuarios ajenos o que deberían estar inactivos
	Pérdida de la Integridad				Eliminación de información no autorizada por parte de usuarios no identificados, suplantación o usuario

					s que deberían estar inactivos.
	Pérdida de la Disponibilidad				Acceso a la información por parte de personas no autorizadas por la falta de seguimiento de un procedimiento formal.
Persona	Pérdida de la Confidencialidad	Falta de mecanismos de monitoreo	Interceptación de información - Espionaje	Falta de seguimiento de los usuarios autorizados a los sistemas de información.	Acceso a información clasificada y reservada a personal no aut

					oriz ado .
Persona	Pérdida de la Confidencialidad	Falta de mecanismos de monitoreo	Robo de medios, equipos o documentos.	Eliminación de datos de los sistemas de información sin autorización por parte de personal sin usuarios a los sistemas de información.	Falta de acceso a sistemas de información o a documentos Persona debido a su robo.
	Pérdida de la Disponibilidad				
Persona	Pérdida de la Integridad	Falta de mecanismos de monitoreo	Manipulación de información	Modificación de información sin autorización en los sistemas de información.	Reportes de información alterada que puedan generar riesgos de cumplimiento legal

Persona	Pérdida de la Confidencialidad	Falta de mecanismos de monitoreo	Repudio de acciones	No aceptación de recepción o envío de comunicaciones.	Falta de controles en los canales de comunicación que permitan mantener la trazabilidad de los registros de envío y recepción de información
	Pérdida de la Integridad				Modificación en las comunicaciones que no garantice n el repudio.

Persona	Pérdida de la Confidencialidad	Inadecuada supervisión de proveedores externos	Abuso de derechos o autorizaciones	No revisar los accesos de los proveedores e identificar los puntos de acceso.	Acceso a los sistemas de información de personas no autorizadas o en horarios no autorizados
	Pérdida de la Integridad				Eliminación de información sin autorización o falta de disponibilidad de los sistemas de información

	Pérdida de la Disponibilidad				Acceso de personas no autorizadas a información clasificada o reservada de la entidad
Persona	Pérdida de la Integridad	Inadecuada supervisión de proveedores externos	Manipulación de información	Modificaciones de información de manera involuntaria y no autorizada.	Modificaciones a la información institucional sin autorización
Persona	Pérdida de la Confidencialidad	Inadecuado nivel de conocimiento y/o concienciación de servidores públicos	Ingeniería Social	Falta de conocimientos del personal de condiciones de seguridad de la información.	Que terceros tengan acceso a la información de usuario y contraseña

					sin autorización.
	Pérdida de la Integridad				Modificaciones en los sistemas de información no autorizadas y con usuarios no propios.
Pers	Pérdida de la Confidencialidad	Inadecuado nivel de conocimiento y/o	Error de uso, uso o administración	Errores en el uso de sistemas de informaci	Modificaciones en los sistemas de información no programadas o no autorizadas, debido a la falta

o n a		concie nciaci ó n de emple ados	incorr ectos de dispo sitivos y siste mas	ón.	de conoc imient o en el manej o de los siste mas de infor maci ón.
	Pé rdi da de la Int eg rid ad				Elimin ación de inform ación de mane ra involu ntaria o restric ción a los acces os de inform ación de ma ner a no aut oriz ada
	Pé rdi da de la Di sp oni bili da d				Us o de los sistem as inform ación por parte de perso nas autori zadas que no de no o

					tienen una adecuada segregación de funciones.
Organizacional	Pérdida de la Integridad	Ubicación susceptible a pérdidas de agua	Daños por agua	Afectación de los sistemas de información cuando ingresa agua a los centros de procesamiento o almacenamiento	Modificaciones en el procesamiento de información
	Pérdida de la Disponibilidad				Falta de disponibilidad a los sistemas de información por fallos en sus dispositivos o componentes.

Organizacional	Pérdida de la Confidencialidad	Falta de procedimientos de identificación y evaluación de riesgos	Mala planeación o falta de adaptación	Falta definir el procedimiento de gestión de usuarios que incluya varios controles de seguridad en acceso a la información.	Usuarios no autorizados en los sistemas de información.
	Pérdida de la Integridad				Modificaciones de información de usuarios no autorizados
	Pérdida de la Disponibilidad				Eliminación de información no autorizada o falta de acceso a los sistemas de información a usuarios autorizados

Organizacional	Pérdida de la Disponibilidad	Falta de un proceso formal para la autorización de la información pública disponible.	Violación de leyes o regulaciones	Definición de la información pública y el momento de su publicación en caso de ser necesario.	Personas no autorizadas con acceso a información.
	Pérdida de la Integridad			La falta de identificación y autorización de ingreso de visitantes	Perdida de información almacenada en medios externos o equipos que no pueda ser recuperada

Instalaciones	Pérdida de la Confidencialidad	Acceso no restringido a instalaciones	Manipulación de hardware o software	Visitantes que accedan a los equipos de la entidad sin autorización	Personas no autorizadas con acceso a equipos de la entidad con usuarios abiertos y que puedan acceder a información confidencial del usuario.
	Pérdida de la Integridad				Modificaciones a la información sin autorización.

	Pérdida de la Disponibilidad				Eliminación de información no autorizada u ocupación.
Instalaciones	Pérdida de la Disponibilidad	Ubicación susceptible a desastres naturales	Desastre natural	Presentación de un desastre natural que afecte las instalaciones de tratamiento de la información.	Destrucción de los equipos o daño de los equipos en los que se realiza tratamiento de información.
Persona	Pérdida de la Disponibilida	Ausencia de personal	Desastre ambiental	Como el caso de la pandemia debido al COVID – 19 donde se tomaron medidas de restricción en la movilidad	Falta de información a la ciudadanía o a los

	d			de las personas	entes de control de forma oportuna.
	Pérdida de la Disponibilidad		Desastre natural	Presentación de un desastre natural que afecte la capacidad de asistencia de los servidores a las instalaciones de la entidad.	
	Pérdida de la Disponibilidad		Fenómenos climáticos y meteorológicos os	Debido a factores climatológicos o meteorológicos los servidores de la entidad no puedan asistir a las instalaciones	
	Pérdida de la Confidencialidad	Copiado sin control	Divulgación de información confidencial	Dejar documentos en los centros de impresión y copiado	Personas no autorizadas puedan acceder a la

Información					información no custodiada
	Pérdida de la Confidencialidad	Nivel de confidencialidad ad no definido con claridad		La falta de clasificación de la información no permitirá definir los controles necesarios para su seguridad.	Información con controles de seguridad no acordes a su nivel de clasificación.
	Pérdida de la Integridad		Violación de leyes o regulaciones		Personas no autorizadas con acceso a la información clasificada y reservada.
	Pérdida de la				Modificaciones no autorizadas de

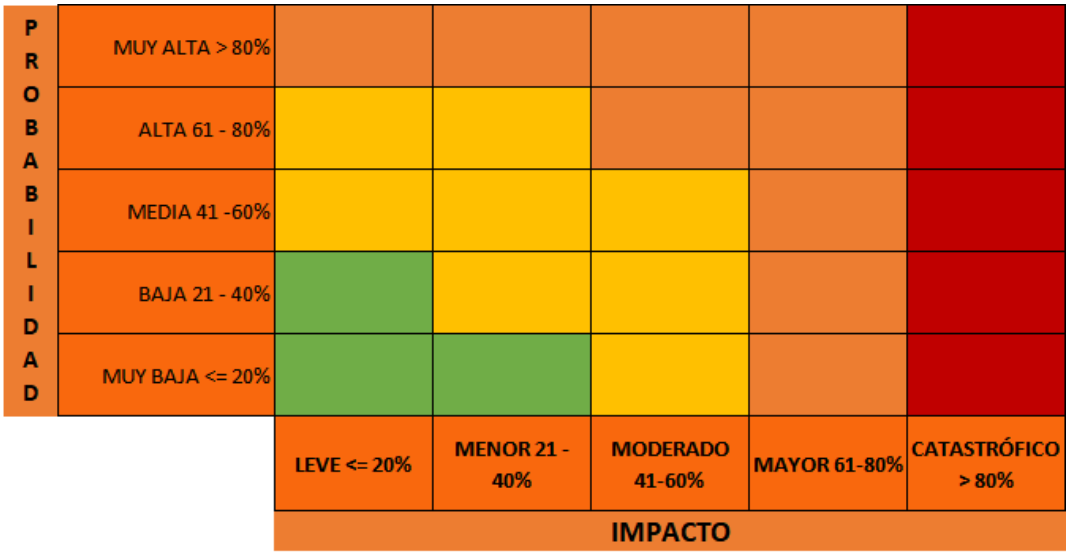
	Disponibilidad dad				información.
					Eliminación de información sin autorización que pueda ser requerida por un organismo de control.
Información	Pérdida de la Confidencialidad	Reglas para control de acceso no definidos con claridad	Abuso de derechos o autorizaciones s	Personas con mayores accesos a la información que los autorizados	Acceso a información no autorizada.
	Pérdida de la Integridad				Modificaciones no autorizadas a información a

					la cual no debería tener acceso el usuario
	Pérdida de la Disponibilidad				Eliminación no autorizada de información.
información	Pérdida de la Integridad	Reglas para control de acceso no definidos con claridad	Manipulación de información	Servidores o terceros con accesos a información no autorizada por parte de la entidad	Modificaciones o cambios en el procesamiento de información sin autorización.
información	Pérdida de la Disponibilidad	Única copia, sólo una copia de la información	Perdida de medios, equipos o documentos	Destrucción o daño físico de la única copia de información	Perdida completa o parcial del repositorio de información.

Fuente: https://www.bomberosbogota.gov.co/sites/default/files/documentos/TIC-PL02%20Plan%20de%20Tratamiento%20de%20Riesgos%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informaci%C3%B3n.pdf

EVALUACIÓN DEL RIESGO

La evaluación de riesgos es el proceso de determinar la probabilidad y el impacto de los riesgos identificados en la seguridad y privacidad de la información. Se realiza para priorizar los riesgos y centrarse en los más críticos.



EXTREMO	
ALTO	
MODERADO	
BAJO	

ANALISIS DE RIESGO

Palabras clave para comprender el procedimiento que se espera seguir en el análisis de riesgos:

Asumir: Significa que la organización reconoce el riesgo, pero decide aceptarlo sin implementar medidas específicas de mitigación. Esto puede ser apropiado cuando el costo de implementar medidas de control supera los posibles daños del riesgo.

Transferir: Implica transferir el riesgo a otra parte, generalmente a través de seguros u otros acuerdos contractuales. En lugar de manejar directamente el riesgo, la organización se protege compartiendo la responsabilidad con terceros.

Mitigar: Se refiere a la acción de implementar controles o medidas para reducir la probabilidad o el impacto de un riesgo. El objetivo es minimizar el riesgo a un nivel aceptable.

Evitar: Esta medida implica tomar acciones para eliminar por completo el riesgo, por lo general evitando la actividad o situación que podría dar lugar al riesgo en primer lugar.

Aceptar: Significa que la organización reconoce el riesgo, pero decide no tomar ninguna medida específica para gestionarlo. Esto puede ser apropiado cuando el riesgo es bajo o insignificante.

Transferir: Consiste en trasladar la responsabilidad del riesgo a otra entidad, como un proveedor de servicios o un tercero, mediante contratos o acuerdos específicos.

Diversificar: En algunos casos, la organización puede optar por diversificar sus activos o actividades para reducir la exposición a un solo riesgo.

Preparar: Esto implica la preparación y planificación de cómo responder a un riesgo si se materializa. Esto puede incluir planes de continuidad del negocio, planes de respuesta a incidentes, etc.

SEMAFORO	BAJO		MODERADO	
	ALTO		EXTREMO	

ANÁLISIS DE RIESGOS EN EL C.O.B.D

ACTIVO	RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	ANALISIS RIESGO	MEDIDAS DE RESPUESTA
Red WiFi	Pérdida de la Confidencialidad, Integridad o Disponibilidad	Acceso no autorizado a la red WiFi	Contraseñas débiles o falta de encriptación	35	40	MODERADO	Evitar
Programa de Computador Contabilidad	Pérdida de la Integridad o Disponibilidad	Ataque de malware o falla enel servidor de contabilidad	Falta de actualizaciones de seguridad en el servidor	30	45	MODERADO	Preparar
Programa de Emergencias	Pérdida de la Integridad o Disponibilidad	Fallo en el programa de emergencias durante una situacióncrítica	Falta de pruebas y mantenimiento del programa	30	35	MODERADO	Mitigar

Programa de Presupuesto	Pérdida de la Integridad o Disponibilidad	Corrupción de datos o falla en el servidor de presupuesto	Falta de respaldo regular de datos presupuestarios	25	40	MODERADO	Mitigar
Programa de Orden del Día	Pérdida de la Integridad o Disponibilidad	Corrupción de datos o falla en el servidor de órdenes del día	Falta de respaldo regular de los datos de órdenes del día	25	40	MODERADO	Mitigar
Servidor de Contabilidad	Pérdida de la Disponibilidad	Falla del servidor debido a su antigüedad	Falla por obsolescencia y recursos limitados del servidor	45	60	ALTO	Evitar
Red (Cableado Estructurado)	Pérdida de la Confidencialidad, Integridad o Disponibilidad	Acceso no autorizado a la red por personal no autorizado	Falta de controles de acceso adecuados	25	55	MODERADO	Evitar
Personal de la Empresa (Con Poco Entrenamiento en Seguridad de Datos)	Pérdida de la Confidencialidad o Integridad	Acceso no autorizado o mal uso de datos	Falta de concientización y capacitación en seguridad de datos	55	40	MODERADO	Preparar

Página Web	Pérdida de la Disponibilidad o Integridad	Ataques cibernéticos que causen la caída del sitio web o la modificación no autorizada de contenidos	Falta de protección contra ataques web y actualizaciones de seguridad	20	60	MODERADO	Transferir
Instalaciones	Daño físico a las instalaciones	Desastres naturales (sismos, incendios)	Falta de medidas de seguridad física	30	45	MODERADO	Preparar
Riesgos Naturales (Sismos)	Daño a activos físicos y sistemas	Terremotos	Falta de medidas de mitigación y planes de contingencia	45	50	MODERADO	Preparar

PLAN DE MITIGACIÓN DE RIESGOS

PLAN DE MITIGACIÓN DE RIESGOS									
Riesgo	Amenaz	Vulner	Probabi	Impacto	Análisi	Acciones de Mi	Respon	Fecha de	Fecha de F	Estado

	a	abilidad	lidad (%)	(%)	sdeRiesgo	tigación	sable	Inicio	inalización	
SISTEMA CONTABLE BASE DE DATOS (Hardware)	Falla del servidor debido a su antigüedad	Falla por obsolescencia y recursos limitados del servidor	50	60	Alto	Compra de equipo nuevo con el lleno de requisitos para que soporte las actividades de servidor	Director y responsable de Tecnología	2024	2024	Ejecutado
Red WiFi - Pérdida de la Confidencialidad, Integridad o Disponibilidad	Acceso no autorizado a la re	Contraseñas débiles o falta	35	40	Moderado	Cortafuegos, restricciones de acceso a la red WiFi con reglas de segu	Responsabled	2024	2024	Ejecutado

	dWiFi	deencriptación				ridad en autenticación y limitación de navegación local	etecnología			
Programa de Computador Contabilidad Pérdida de la Integridad o Disponibilidad	Ataque de malware o falla en el servidor de contabilidad	Falta de actualizaciones de seguridad en el servidor	30	45	Moderado	Mantener actualizado el programa antivirus con licencia en los computadores de la entidad	Responsable de tecnología	2024	2024	Ejecutado
Programa de Emergencias - Pérdida de la Integridad o Disponibilidad	Fallo en el programa de emer	Falta de pruebas y manteni	30	35	Moderado	Realizar copias de seguridad diarias	Responsable de	2024	2024	Ejecutado

	gencias durante una situación crítica	miento del programa					tecnología			
Programa de Presupuesto - Pérdida de la Integridad o Disponibilidad	Corrupción de datos o falla en el servidor de presupuestos	Falta de respaldo regular de datos presupuestarios	25	40	Moderado	Realizar copias de seguridad diarias	Responsable de tecnología	2024	2024	Ejecutado
Programa de Orden del Día - Pérdida de la Integridad o	Corrupción de datos o	Falta de respaldo regular	25	40	Moderado	Realizar copias de seguridad diarias	Responsabl	2024	2024	Ejecutado

Disponibilidad	falla en el servidor de órdenes del día	de los datos de órdenes del día					detección tecnología			
Red (Cableado Estructurado) - Pérdida de la Confidencialidad, Integridad o Disponibilidad	Acceso no autorizado a la red por personal no autorizado	Falta de controles de acceso adecuados	25	55	Moderado	Puntos físicos de datos desconectados si no tienen uso, firewall y bloqueo en cortafuegos	Responsable de tecnología	2024	2024	Ejecutado

Personal de la Empresa (Con Poco Entrenamiento en Seguridad de Datos) - Pérdida de la Confidencialidad o Integridad	Acceso no autorizado o mal uso de datos	Falta de concientización y capacitación en seguridad de datos	55	40	Moderado	Brindar capacitación al personal de la Institución sobre reglas básicas de protección de datos personales y de la empresa	Responsable de tecnología	2024	2024	Ejecutado
Página Web - Pérdida de la Disponibilidad o Integridad	Ataques cibernéticos que causen la caída del sitio w	Falta de protección contra ataques web y actualizacio	20	60	Moderado	Verificar que el Hostingcumpla con los requisitos de seguridad y respaldo de servicio, se debe cam	Responsable de tecnolog	2024	2024	Ejecutado

	ebo la modificación no autorizada de contenidos	nes de seguridad				biar si no es seguro	ía			
Instalaciones - Daño físico a las instalaciones	Desastres naturales (sismos, incendios)	Falta de medidas de seguridad física	30	45	Moderado	Copia de seguridad en la nube de programas y bases de datos	Responsable de tecnología	2024	2026	Planificado
Riesgos Naturales (Sismos) - Daño a	Terremotos	Falta de medidas de	45	50	Modera	Copia de seguridad en la nube de prog	Respons	2024	2025	Planif

activos físicos y sistemas		mitigación y planes de contingencia			do	ramas y bases de datos	able de tecnología			icado
sistema contable – base de datos (hardware / Software)	Indisponibilidad del sistema contable	Dependencia de infraestructura local con recursos limitados y sin alta disponibilidad	40	60	Alto	Evaluar la implementación de esquemas de respaldo y recuperación en entornos de computación en la nube (Cloud First), garantizando la disponibilidad y continuidad del sistema contable.	Responsable de tecnología	2026	2027	Planificado

información institucional (Base de datos y documentos)	Pérdida o corrupción de información	Respaldos insuficientes o no verificados periódicamente	45	70	Alto	Implementar y probar periódicamente esquemas de copias de seguridad locales y en la nube, incluyendo procedimientos documentados de restauración de la información.	Responsable de tecnología	2026	2026	Planificado
seguridad de la información (uso de herramientas tecnológicas)	Exposición de información sensible o datos personales	Uso inadecuado de herramientas de inteligencia artificial sin lineamient	35	70	Alto	Definir e implementar lineamientos institucionales para el uso responsable de herramientas de inteligencia	Responsable de tecnología	2026	2026	Planificado

		os institucionales				artificial, prohibiendo el uso de información sensible o datos personales y capacitando al personal.				
riesgo existente de accesos y usuarios (softwares nuevos)	Acceso no autorizado a sistemas de información	Asignación inadecuada de perfiles y credenciales en nuevos aplicativos o software institucional	40	65	Alto	Revisar y controlar la asignación de perfiles de usuario en los sistemas de información y software institucional, aplicando el principio de míni	Responsable de tecnología	2026	2027	Planificado

						mo privilegio.				

CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Controles de Seguridad y Privacidad de la Información

Control	Descripción del Control	Responsable	Fecha de Implementación	Estado
Hardware	Actualizar el servidor antiguo por uno nuevo y más robusto	Director y responsable de Tecnología	2024	Ejecutado
Red WiFi	Implementar cortafuegos y reglas de seguridad en autenticación	Responsable de tecnología	2024	Ejecutado

Programa de Computador Contabilidad	Mantener actualizado el programa antivirus en los computadores	Responsable de tecnología	2024	Ejecutado
Programa de Emergencias	Realizar copias de seguridad diarias	Responsable de tecnología	2024	Ejecutado
Programa de Presupuesto	Realizar copias de seguridad diarias	Responsable de tecnología	2024	Ejecutado
Programa de Orden del Día	Realizar copias de seguridad diarias	Responsable de tecnología	2024	Ejecutado
Red (Cableado Estructurado)	Desconectar puntos físicos de datos sin uso y mejorar cortafuegos	Responsable de tecnología	2024	Ejecutado

Personal de la Empresa (Con Poco Entrenamiento en Seguridad de Datos)	Brindar capacitación sobre protección de datos	Responsable de tecnología	2024	En proceso
Página Web	Verificar que el Hosting cumpla con requisitos de seguridad	Responsable de tecnología	2024	Ejecutado
Instalaciones	Realizar copias de seguridad en la nube de programas y bases de datos	Responsable de tecnología	2025	Planificado
Riesgos Naturales (Sismos)	Realizar copias de seguridad en la nube de programas y bases de datos	Responsable de tecnología	2025	Planificado

Uso de Herramientas de Inteligencia Artificial	Establecer lineamientos institucionales para el uso responsable de herramientas de inteligencia artificial, evitando el uso de información sensible o datos personales.	Responsable de tecnología	2026	Planificado
Gestión de Proveedores Tecnológicos	Evaluar que los proveedores tecnológicos cumplan con requisitos mínimos de seguridad de la información y privacidad.	Responsable de tecnología	2026	Planificado
Evaluación de Servicios en la Nube	Realizar la evaluación de alternativas de servicios en la nube bajo el enfoque Cloud First, definiendo	Responsable de tecnología	2026	Planificado

	lineamientos mínimos de seguridad y privacidad de la información para una eventual adopción futura.			

POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD

POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD					
Tipo	**Nombre de la Política/Procedimiento**	**Descripción**	**Fecha de Implementación**	**Responsable**	**Estado**
Política	Política de Acceso y Autenticación	Procedimientos para garantizar un acceso seguro y autenticación adecuada.	2025	Responsable TIC	Planificado
Política	Política de Respaldo de Datos	Procedimientos para realizar copias de seguridad diarias de datos críticos.	2024	Responsable TIC	Implementado

Política	Política de Capacitación en Seguridad	Capacitación al personal sobre reglas básicas de protección de datos.	2025	Responsable TIC	Planificado
Procedimiento	Procedimiento de Actualización de Software	Mantenimiento del software antivirus en los computadores.	2024	Responsable TIC	Ejecutado
Procedimiento	Procedimiento de Seguridad Física de Instalaciones	Medidas de seguridad física, como copia de seguridad en la nube.	2025	Responsable TIC	En proceso
Procedimiento	Procedimiento de Gestión de Incidentes	Especifica cómo se deben detectar, reportar y responder a los incidentes de seguridad de la información.	2025	Responsable TIC	Planificado

Procedimiento	Procedimiento de Evaluación de Riesgos	Detalla cómo se llevará a cabo la evaluación periódica de riesgos de seguridad de la información, incluyendo la identificación de amenazas, vulnerabilidades y la evaluación de la probabilidad e impacto de los riesgos	2025	Responsable TIC	Planificado
Política	Política de Uso de Herramientas de Inteligencia Artificial	Establece lineamientos para el uso responsable de herramientas de	2026	Responsable TIC	Planificado
		inteligencia artificial, garantizando la seguridad y privaci			

		dad de la información institucional.			
Procedimiento	Procedimiento de Gestión de Proveedores Tecnológicos	Definir los pasos para evaluar y controlar a los proveedores tecnológicos, verificando el cumplimiento de requisitos de seguridad y privacidad de la información.	2026	Responsable TIC	Planificado

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES:

Objetivo: Describir el proceso para gestionar eficazmente los incidentes de seguridad de la información y minimizar su impacto en la organización.

Alcance: Este procedimiento se aplica a todos los incidentes de seguridad de la información en la organización, incluyendo aquellos relacionados con la confidencialidad, integridad y disponibilidad de datos.

Este procedimiento también aplica a incidentes asociados al uso de herramientas de inteligencia artificial, servicios tecnológicos en la nube y proveedores externos de servicios TIC.

Responsabilidades:

El Equipo de Respuesta a Incidentes (ERI) es responsable de coordinar y gestionar la respuesta a incidentes.

El responsable de Tecnología es responsable de supervisar y apoyar las acciones del ERI.

Todos los empleados son responsables de reportar incidentes de seguridad de la información de inmediato al ERI.

Procedimiento:

Detección del Incidente:

Todo el personal debe estar alerta ante posibles incidentes de seguridad y reportar cualquier anomalía o incidente sospechoso al ERI.

El ERI puede utilizar sistemas de monitoreo de seguridad para detectar incidentes de forma proactiva.

Reporte del Incidente:

- ✓ Cualquier empleado que detecte o sospeche un incidente debe notificarlo de inmediato al ERI a través de los canales de comunicación designados.
- ✓ El ERI debe registrar la información inicial del incidente, incluyendo la fecha, hora, descripción y cualquier detalle relevante.

Evaluación y Clasificación del Incidente:

- ✓ El ERI evaluará la gravedad y el alcance del incidente para determinar su clasificación (por ejemplo, baja, moderada o alta).
- ✓ Se utilizarán criterios predefinidos para clasificar el incidente en función de su impacto potencial.

Análisis del Incidente:

- ✓ El ERI llevará a cabo un análisis detallado del incidente para determinar su causa raíz, método de ataque, vectores de ataque y posibles efectos en la organización.
- ✓ Se recopilarán evidencias y registros relevantes.

- ✓ Respuesta al Incidente:
- ✓ Basándose en la clasificación del incidente y su análisis, el ERI desarrollará un plan de respuesta que incluya medidas para contener, mitigar y resolver el incidente.
- ✓ Se identificarán las acciones específicas a tomar, como la eliminación de malware, la restauración de datos o la notificación a las partes interesadas.
- ✓ En caso de incidentes relacionados con servicios en la nube, herramientas de inteligencia artificial o proveedores tecnológicos, se deberá identificar la responsabilidad del tercero y aplicar los acuerdos contractuales y de nivel de servicio correspondientes.

Comunicación y Notificación:

- ✓ Se notificará a las partes interesadas relevantes sobre el incidente, incluyendo la alta dirección, los empleados afectados y las autoridades pertinentes, si es necesario.
- ✓ La comunicación se realizará de manera oportuna y siguiendo los requisitos legales y normativos.

Registro y Documentación:

- ✓ Se mantendrá un registro detallado de todas las acciones tomadas durante la gestión del incidente, incluyendo los resultados del análisis, las medidas implementadas y las comunicaciones realizadas.

Evaluación Post-Incidente:

- ✓ Una vez que el incidente esté resuelto, se llevará a cabo una revisión post-incidente para evaluar la efectividad de las medidas tomadas y determinar lecciones aprendidas.
- ✓ Se actualizará la documentación y se implementarán mejoras si es necesario. Cierre del Incidente:
- ✓ El ERI declarará formalmente el cierre del incidente una vez que se hayan completado todas las acciones y se haya confirmado que la amenaza se ha mitigado.

- ✓ ***Procedimiento de Control de Acceso*****:** Describe cómo se administrarán y controlarán los accesos a sistemas y datos confidenciales, incluyendo la creación y eliminación de cuentas de usuario, la gestión de contraseñas y las políticas de autenticación.

- ✓ ***Procedimiento de Respuesta a Emergencias***: Detalla cómo se debe actuar en situaciones de emergencia que puedan afectar la seguridad de la información, como desastres naturales o cibernéticos. Describe los pasos para garantizar la continuidad de las operaciones.

- ✓ ***Procedimiento de Copias de Seguridad***: Especifica cómo se realizarán las copias de seguridad de datos críticos, con qué frecuencia se realizarán, dónde se almacenarán y cómo se restaurarán en caso de pérdida de datos.

- ✓ ***Procedimiento de Evaluación de Riesgos***: Detalla cómo se llevará a cabo la evaluación periódica de riesgos de seguridad de la información, incluyendo la identificación de amenazas, vulnerabilidades y la evaluación de la probabilidad e impacto de los riesgos.

PROCEDIMIENTO DE EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Objetivo:

El objetivo de este procedimiento es establecer las pautas para la identificación, análisis, evaluación y gestión de los riesgos de seguridad de la información en
C.O.B.D. Esto incluye la determinación de las amenazas, vulnerabilidades, impacto y probabilidad de los riesgos, así como la implementación de medidas de mitigación y el seguimiento continuo de los riesgos identificados.

Alcance:

Este procedimiento se aplica a todos los activos de información y procesos de C.O.B.D, incluidos los sistemas de información, datos confidenciales y cualquier otro activo relacionado con la seguridad de la información.

Responsabilidades:

El responsable de las TIC es el encargado de supervisar y coordinar la evaluación de riesgos de seguridad de la información.

El responsable de las TIC es el responsable de proporcionar información y apoyo para la evaluación de riesgos de los activos bajo su responsabilidad.

Procedimiento:

Identificación de Activos y Valoración:

El equipo de evaluación de riesgos identificará y catalogará todos los activos de información críticos para la entidad, incluyendo sistemas, datos, infraestructuras y procesos.

Cada activo será valorado en función de su importancia para la entidad y su impacto potencial en caso de una amenaza.

Identificación de Amenazas y Vulnerabilidades:

Se identificarán todas las amenazas que puedan afectar a los activos de información, considerando tanto amenazas internas como externas.

Se identificarán las vulnerabilidades asociadas a cada activo, incluyendo debilidades en los controles de seguridad existentes.

Se considerarán riesgos emergentes asociados al uso de nuevas tecnologías, tales como servicios en la nube, herramientas de inteligencia artificial y la dependencia de proveedores tecnológicos.

Análisis de Riesgos:

Se determinará la probabilidad de que ocurra cada amenaza y se evaluará el impacto potencial en los activos afectados.

Se calculará el nivel de riesgo para cada combinación de amenaza y activo.

Evaluación de Riesgos:

Se priorizarán los riesgos identificados en función de su nivel de riesgo, considerando tanto la probabilidad como el impacto.

Los riesgos se clasificarán en categorías como Extremo, alto, Moderado y Bajo.

Implementación de Medidas de Mitigación:

Para los riesgos identificados como "Alto", se diseñarán e implementarán medidas de mitigación adecuadas. Esto puede incluir la implementación de controles de seguridad adicionales, actualizaciones de sistemas o cambios en los procesos.

Se asignará un responsable para cada medida de mitigación, y se establecerán fechas de inicio y finalización.

Seguimiento y Revisión:

Los riesgos y las medidas de mitigación se revisarán de forma periódica para asegurarse de que sigan siendo relevantes y efectivos.

Se actualizarán los registros de riesgos y las medidas de mitigación según sea necesario.

Comunicación y Formación:

Se informará a los empleados y partes interesadas relevantes sobre los riesgos de seguridad de la información y las medidas de mitigación implementadas.

Se proporcionará formación sobre seguridad de la información según sea necesario.

Registro de Riesgos:

Se mantendrá un registro actualizado de todos los riesgos identificados, las medidas de mitigación y su estado.

Documentación y Registro:

Se mantendrá documentación detallada de todas las actividades de evaluación de riesgos, incluyendo registros de activos, amenazas, vulnerabilidades, riesgos,

medidas de mitigación y revisiones.

POLÍTICA DE RESPALDO DE DATOS

1. Propósito:

La presente política tiene como objetivo establecer las directrices y procedimientos para la realización de respaldos de datos de manera segura y eficiente en C.O.B.D, con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información crítica de la organización.

2. Alcance:

Esta política es de aplicación a todos los empleados, contratistas y terceros que manejen o tengan acceso a la información de C.O.B.D, así como a todos los sistemas y activos de información de la organización.

3. Responsabilidades:

El responsable de tecnología o TIC será el encargado de supervisar y administrar el proceso de respaldo de datos.Cada área o departamento designará un responsable de respaldo de datos para garantizar la ejecución de los procedimientos de acuerdo con esta política.

4. Procedimiento de Respaldo de Datos:

4.1 Identificación de Datos Críticos:

Se identificarán y catalogarán los datos críticos y sistemas de información que requieran ser respaldados regularmente. Esto incluye, pero no se limita a, bases de datos, archivos de configuración, documentos importantes y registros de transacciones.

4.2 Frecuencia de Respaldo:

Se establecerán intervalos de respaldo de acuerdo con la criticidad de los datos. Los datos críticos deberán respaldarse con mayor frecuencia.

4.3 Métodos de Respaldo:

Se utilizarán métodos de respaldo seguros y confiables, como copias de seguridad en cinta, almacenamiento en la nube o dispositivos de almacenamiento externo.

El uso de almacenamiento en la nube estará sujeto a evaluación previa de seguridad, disponibilidad y cumplimiento normativo, y se realizará conforme a la planeación y priorización institucional.

Se garantizará que los datos respaldados estén protegidos contra accesos no autorizados y ataques cibernéticos.

4.4 Retención de Copias de Seguridad:

Se establecerán políticas de retención que definan cuánto tiempo se deben conservar las copias de seguridad. Esto dependerá de los requisitos legales y comerciales.

4.5 Pruebas de Restauración:

Se realizarán pruebas periódicas de restauración para verificar la integridad de las copias de seguridad y la capacidad de recuperación de los datos en caso de desastres.

4.6 Registro de Respaldo:

Se llevará un registro detallado de todas las operaciones de respaldo, incluyendo fechas, tipos de datos respaldados y resultados de las pruebas de restauración.

5. Cumplimiento y Auditoría:

El cumplimiento de esta política será supervisado y auditado de forma regular por el responsable de las TIC en el C.O.B.D.

6. Formación y Concienciación:

Se proporcionará formación y concienciación sobre la política de respaldo de datos a todos los empleados y partes interesadas involucradas en el proceso.

7. Revisiones y Actualizaciones:

Esta política será revisada y actualizada periódicamente para garantizar su relevancia y eficacia.

8. Sanciones por Incumplimiento:

El incumplimiento de esta política puede resultar en medidas disciplinarias de acuerdo con las políticas internas de C.O.B.D, así como en responsabilidad legal en caso de pérdida de datos críticos.

CONTROL DE CAMBIOS Y ACTUALIZACIÓN DOCUMENTAL

FECHA	VERSIÓN	DESCRIPCIÓN	RESPONSABLE
30/01/2026	2	➢ En la introducción se ajusta la información para la vigencia 2026. ➢ Se modificaron los 2 últimos objetivos específicos. ➢ Se agrega el punto 8.1 al documento. ➢ A la tabla plan de mitigación de riesgos se anexan los 4 últimos registros. ➢ Se agrega a la tabla de controles de seguridad y privacidad de la información los últimos 3 registros. ➢ En procedimiento de gestión de incidentes se actualiza alcance. ➢ Se modifico modifico de forma general los procedimientos del documento	JOHSON BETANCUR

ELABORADO POR:	REVISADO POR:	APROBADO POR:
JOHSON BETANCUR	ERICA CARDENAS SANDRA L. GIRALDO	JOSE JOAQUIN OCAMPO P
TICS	Calidad - MIPG	Director general