[Honor, Valor, Disciplina]

U.A.E. CUERPO OFICIAL BOMBEROS BOGOTÁ D.C.

PLAN DE TRATAMIENTO DE RIESGOS

Versión: 2-2026

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ

Tabla de contenido

1. INTRODUCCIÓN

La información tratada en una entidad pública es fundamental para cumplir con sus objetivos misionales, en este sentido la Unidad Administrativa Especial del Cuerpo de bomberos de Bogotá ha declarado su compromiso con la seguridad y privacidad de la información mediante la aprobación de la Política de Seguridad, la cual se operativiza con el Manual de Seguridad y Privacidad de la Información, el cual presenta para el usuario final y los diferentes roles que intervienen en los procesos de producción y manejo de información los controles que adopta la entidad para el manejo de la información basado en los dominios que plantea la norma técnica ISO 27001:2013.

El nivel de madurez de implementación del Modelo de Seguridad y Privacidad de la Información - MPSI, en la Unidad corresponde al **nivel 1 Inicial**, lo que implica que: a) Se han identificado las debilidades en la seguridad de la información. b) Los incidentes de seguridad de la información se tratan de forma reactiva. c) Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.

La metodología adoptada para la gestión de riesgos de seguridad de la información está definida en la norma técnica ISO 27005 y que se encuentra perfectamente alineada con la metodología propuesta por el DAFP.

2. OBJETIVO

Implementar una herramienta para la gestión de riesgos de Seguridad y Privacidad de la información con el fin de preservar la confidencialidad, integridad y disponibilidad de la información y desarrollar de manera adecuada los procesos misionales, estratégicos y administrativos.

3. ALCANCE

Teniendo en cuenta que el nivel de madurez de implementación del Modelo de Seguridad y Privacidad de la Información en la Entidad está en nivel **Efectivo,** el plan de gestión del riesgo asociado a los activos de información adelantara el levantamiento de activos de información, la clasificación, etiquetado y priorización de estos para poder iniciar con la gestión del riesgo.

4. RESPONSABLE

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

5. MARCO NORMATIVO

Marco Normativo	Descripción
Decreto 510 de 2023	Por medio del cual se modifica la planta de empleos de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos.
8Decreto Nº 509 de 2023	"Por Medio del cual se Modifica la Estructura Organizacional de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos."
Decreto 359 de 2022	Por medio del cual se modifica el Decreto Distrital 555 de 2011 "Por medio del cual se modifica la estructura organizacional de la Unidad Administrativa Cuerpo Oficial de Bomberos y se dictan otras disposiciones".
Decreto 360 de 2022	Por medio del cual se modifica el Decreto 559 de 2011 "Por el cual se establece la planta de cargos de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá. D.C. li, se dictan otras disposiciones."
Ley 962 de 2005	"Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos."
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.

Marco Normativo	Descripción
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1955 del 2019	Establece que las Entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
Decreto 2150 de 1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Decreto 025 de 2021	Por medio del cual se reglamenta la Comisión Distrital de Transformación Digital.
Decreto 619 de 2007	Se establece la Estrategia de Gobierno Electrónico de los organismos y de las Entidades de Bogotá, Distrito Capital y se dictan otras disposiciones.
Decreto 185 de 2008.	Por el cual se prorroga el plazo para formular la Estrategia Distrital de Gobierno Electrónico de los organismos y de las Entidades de Bogotá, Distrito Capital.
Decreto 296 de 2008.	Por el cual se le asignan las funciones relacionadas con el Comité de Gobierno en Línea a la Comisión Distrital de Sistemas y se dictan otras disposiciones en la materia.
Decreto 316 de 2008.	Por medio del cual se modifica parcialmente el artículo 3° del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico.
Decreto 1151 de 2008	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre Entidades para el cumplimiento de funciones públicas.

Marco Normativo	Descripción
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1081 de 2015	"Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República."
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.
Decreto 728 2016	“Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico”.
Decreto 728 de 2017	“Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico”.

Marco Normativo	Descripción
Decreto 1413 de 2017	"Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 2106 de 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública. Cap. II Transformación Digital Para Una Gestión Publica Efectiva
Decreto 620 de 2020	"Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
Decreto 088 de 2022	Por el cual se adiciona el Titulo 20 del libro 2 del Decreto Único Reglamentario del sector de las Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3,5 y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.

Marco Normativo	Descripción
Decreto 338 de 2022	Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de las Seguridad Digital y se dictan otras disposiciones.
Decreto 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1263 de 2022	Por el cual se adiciona el Titulo 22 a la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Publica.
Resolución 256 de 2008	Por la cual se establece el reglamento interno de la Comisión Distrital de Sistemas – C.D.S.
Resolución 305 de 2008	Por la cual se expiden políticas públicas para las Entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
Resolución 378 de 2008	Por la cual se adopta la Guía para el diseño y desarrollo de sitios Web de las Entidades y organismos del Distrito Capital
Resolución 473 de 2011	Por la cual se reestructura el Sistema y el comité del sistema Integrado de Gestión de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos.
Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.

Marco Normativo	Descripción
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Resolución 1117 de 2022	"Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital"
Resolución 746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
Resolución 1978 de 2023	Por la cual se adopta la Versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano como el instrumento para implementar el habilitador de arquitectura de la Política de Gobierno Digital y se dictan otras disposiciones
Norma Técnica Colombiana NTC 5854 de 2012	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.
CONPES 3292 de 2004	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.

Marco Normativo	Descripción
CONPES 3854 Política Nacional de Seguridad Digital de Colombia, del 11 de abril de 2016	El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo
CONPES 3920 de Big Data, del 17 de abril de 2018	Política Nacional de Explotación de Datos (Big Data) Este documento CONPES busca sentar las bases para una política pública integral que habilita el aprovechamiento de los datos para generar desarrollo social y económico.
CONPES 3975 de 2019	Tiene como objetivo impulsar la productividad y el bienestar de los ciudadanos, a través del uso estratégico de las tecnologías digitales en el sector público y privado.
CONPES 3995 de 2020	Por el cual se establece la Política Nacional de Confianza y Seguridad Digital.
CONPES 4023 de 2021	Política para la Reactivación, la Repotenciación y el Crecimiento Sostenible e Incluyente
CONPES 4070 de 2021	Lineamientos de Política para la Implementación de un Modelo de Estado Abierto.
Circular 02 de 2019	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.

Marco Normativo	Descripción
Directiva Distrital 002 de 2002	Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software).
Directiva 005 de 2005	Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital.
Directiva 02 de 2019	Simplificación de la interacción digitalmente los ciudadanos y el estado.
Directiva 005 de 2020	Directrices sobre gobierno abierto de Bogotá de la Alcaldía Mayor de Bogotá.
Directiva 02 de 2022	Las entidades que conforman la administración pública no han sido ajenas a la dinámica propia del incremento de los incidentes en el ámbito cibernético, con el riesgo de producir impactos negativos a partir de la materialización de incidentes de seguridad en el entorno digital. Por ello, la Seguridad Digital es, sin duda alguna, uno de los retos más importantes que enfrentan todo tipo de organizaciones.
Acuerdo 057 de 2002	Por el cual se dictan disposiciones generales para la implementación del sistema Distrital de Información –SDI-, se organiza la Comisión Distrital de Sistemas, y se dictan otras disposiciones.
Acuerdo 130 de 2004	Por medio del cual se establece la infraestructura integrada de datos espaciales para el Distrito Capital y se dictan otras disposiciones.
Acuerdo 279 de 2007	Dicta los lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital.
Acuerdo 409 de 2009	Por el cual se modifica la integración de la Comisión Distrital de Sistemas.

6. MARCO ESTRATÉGICO

Motivador	Fuente
Estrategia Nacional	Plan Nacional de Desarrollo “Colombia potencia mundial de la vida”
	Objetivos de Desarrollo Sostenible Plan TIC Nacional:
	Gobierno digital para la gente. Se diseñará e implementará una estrategia que acelere la digitalización de trámites e impulse el desarrollo de modelos de identidad digital y la masificación de servicios ciudadanos digitales. Asi mismo, se adelantarán ajustes normativos e institucionales que favorezcan la compra y uso inteligente y estratégico de las TIC para proveer productos y servicios innovadores que resuelvan problemáticas y generen valor público.
	Estrategia para el fortalecimiento de la Ciberseguridad. “En respuesta al incremento del conjunto de amenazas cibernéticas que actualmente afectan a las personas, se requiere institucionalizar una hoja de ruta de mediano y largo plazo para el fortalecimiento de las capacidades del ecosistema cibernético nacional en materia de ciberseguridad”.
Estrategia Distrital	Plan Distrital de Desarrollo 2024 al 2027 - El cual involucra en este a la UAECOB, en :
	1°El objetivo 5: “**B***ogotá confía en su gobierno: Lograremos una ciudad pujante, donde uno quiera vivir, requiere de un Gobierno que atienda las necesidades, garantice los derechos de las personas y brinde un servicio amable, ágil y oportuno en todo el territorio con un gasto eficiente. Un gobierno, en el que la ciudadanía crea y confíe.”*
	En la Estrategia 1: Bogotá se fortalece con un gobierno abierto, cercano, eficiente, transparente e íntegro. En el Programa 33: Fortalecimiento institucional para un gobierno confiable.
	Y la meta del Plan de Desarrollo que aplica es un plan para el fortalecimiento de las capacidades institucionales de la UAECOB.”
	“Desarrollar Implementar una red para aumentar la cobertura de capacidades, reducir los tiempos de respuesta y recuperación en la atención emergencias del Cuerpo Oficial de Bomberos en Bogotá Región.
	2° Estructurar un sistema integrado de atención a emergencias y desastres naturales que garantice la capacidad de respuesta frente a los desafíos del cambio climático y reduzca las vulnerabilidades de este en la ciudad región, que contribuyen al Plan de manera directa al cumplimiento de su objetivo general frente a la necesidad de la Entidad.
	Anexo: Anexo 2. Políticas Públicas y POT con el PDDhttps://www.sdp.gov.co/sites/default/files/anexo_2._politicas_publicas_y_pot.xlsx 9Meta PDD 2024 – 2027 Implementar un programa para mejorar la respuesta en la atención a emergencias del Cuerpo Oficial de Bomberos de Bogotá apalancada en redes de conocimiento prevención del riesgo y cobertura en la ciudad y su entorno

Motivador	Fuente
Estrategia Sectorial e Institucional	El Plan Estratégico Institucional de la Unidad Administrativa Especial del Cuerpo Oficial de Bomberos Bogotá (UAECOB) para el periodo 2024 al 2027, Involucra las estrategias del Plan Distrital de Desarrollo:
	Bogotá protege el ambiente y se compromete con la acción climática.
	Bogotá se fortalece con un gobierno abierto, cercano, eficiente, transparente e íntegro.
	Los programas que hacen parte de las estrategias para la UAECOB son:
	Aumento de la resiliencia al cambio climático y reducción de la vulnerabilidad
	Fortalecimiento institucional para un gobierno confiable.
	Metas que hacen parte:
	Implementar un programa para mejorar la respuesta en la atención a emergencias del Cuerpo Oficial de Bomberos de Bogotá, apalancada en redes de conocimiento, prevención del riesgo y cobertura en la ciudad y su entorno.
	Desarrollar un plan para el fortalecimiento de las capacidades institucionales de la UAECOB.
Lineamientos y Políticas	Política de Gobierno Digital
	Marco de la Transformación Digital
	Modelo Integrado de Planeación y Gestión – MIPG
	Entre otros en el marco de la normativa vigente institucional, Función Pública y MINTIC

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 del Estado 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.

Contexto

La Unidad Administrativa Especial Cuerpo de Bomberos de Bogotá es una entidad distrital que tiene como misión *"Proteger la vida, el ambiente y el patrimonio, a través de la gestión integral de riesgos de incendios, atención de rescates en todas sus modalidades e incidentes con materiales peligrosos en Bogotá"* y tiene como visión: *"Al 2030, ser el mejor cuerpo de bomberos de Colombia soportado en el compromiso de sus colaboradores y la confianza de los ciudadanos, reconocido a nivel mundial por su fortaleza técnica y capacidad de gestión*." Teniendo en cuenta que parte de la misión se encuentra soportada en la confianza del ciudadano, el tratamiento de

la información es una de las maneras más importantes para mantener y mejorar la confianza de la ciudadanía en la entidad. Al ser una entidad de carácter público su información se encuentra clasificada de acuerdo con el artículo 6 de la Ley 1712 del 2014 en Información pública, Información pública clasificada e información pública reservada. De esta manera se clasifica la información de la entidad sea en físico o digital.

Gran parte de la información operativa de la entidad es de carácter público por lo cual disminuye su riesgo en relación con la confidencialidad de la información, pero la disponibilidad e integridad de la información para la atención de emergencias puede salvar vidas, por esta razón, la implementación de un modelo de gestión de riesgos en seguridad y privacidad de la información como herramienta que permita a la entidad ser más eficaz y eficiente en la respuesta a emergencias es fundamental para el cumplimiento de su visión. De acuerdo con lo establecido en el Decreto 612 de 2018, la creación del Plan de Tratamiento de Riesgos de Seguridad Digital debe estar alineado con la Planeación Estratégica Institucional y debe ser formulado, aprobado, publicado en la página web institucional y ejecutado de manera anual por cada una de las áreas responsables. Este plan fue elaborado bajo los lineamientos dispuestos por las entidades responsables tales como el Departamento Administrativo de la Función Pública, Ministerio de Tecnologías de la Información y las Comunicaciones, Secretaría de Transparencia, Archivo General de la Nación, entre otros.

El objetivo principal que busca el Plan Estratégico Institucional -PEI- 2024-2027 de la UAECOB es otorgar los lineamientos institucionales y orientadores de la planificación para el presente cuatrienio, basado en 3 ejes estructurales “Proteger-Potenciar-Participar” P3, estableciendo para ello las diferentes acciones estratégicas concertadas año por año en las actividades del Plan de Acción Institucional.

Teniendo en cuenta el P.E.I 2024-2027 el objetivo estratégico del segundo eje estructural “POTENCIAR” y el cual va alineado con tecnología es la Modernizar la gestión y el desempeño institucional a través de la articulación efectiva de los procesos, con innovación pública, transparencia y seguridad de la información para garantizar el equipamiento tecnológico y de infraestructura requerido por la misionalidad.

8. Identificación de amenazas

Las amenazas son los peligros externos que buscan afectar la confidencialidad, integridad o disponibilidad de la información, en la siguiente tabla se describen detalladamente las 37 amenazas más comunes asociadas a la afectación de los 3 principios de seguridad de la información, las cuales están clasificadas en 7 tipos de amenaza.

Las amenazas se han codificado de manera secuencial de 1 a 37 y se anteponen las letras “AM”- para configurar su identificación.

AMENAZAS

Código	Nombre	Descripción	Tipo
AM-01	Fuego - Incendio	El fuego puede causar daños directos y severos a personas, edificaciones o instalaciones, pero también se pueden presentar daños indirectos con consecuencias catastróficas especialmente para las tecnologías de la información. Daños indirectos como los causados por el agua o los químicos usados para combatir el fuego, el humo y los gases producidos por la incineración de elementos, los cuales se pueden diseminar por los conductos de ventilación y dañar equipo electrónico sensible.	Daño físico
AM-02	Daños por agua	El agua puede afectar la integridad y disponibilidad de la información física y digital. Una admisión incontrolada de agua en un edificio o centro de datos puede producirse por Interrupciones en el suministro de agua o eliminación de aguas residuales, Sistemas de aire acondicionado defectuosos con suministro de agua, Sistemas de rociadores defectuosos y agua utilizada en caso de incendio. Independientemente de cómo ingrese el agua en el edificio o centro de datos, conlleva al riesgo que las instalaciones de suministro o los componentes de TI se dañen y salgan de operación (un cortocircuito, daño mecánico, óxido, etc.).	Daño físico

Código	Nombre	Descripción	Tipo
AM-03	Desastre ambiental	Es un accidente grave en el entorno como, por ejemplo, un incendio, una explosión, una liberación de sustancias venenosas o una fuga de radiación peligrosa. Por lo tanto, el peligro no solo se debe al evento en sí, sino a menudo las actividades que resultan de, por ejemplo, restricciones de acceso y medidas de rescate.	Daño físico
AM-04	Contaminación, polvo, corrosión o congelamiento	La acumulación de polvo en los equipos puede generar fallas en su funcionamiento, así mismo la temperatura no controlada puede generar sobrecalentamiento o condensación en los equipos y alterar su funcionamiento	Daño físico
AM-05	Fenómenos climáticos y meteorológicos	Las condiciones climáticas extremas pueden cambiar las condiciones de operatividad de los equipos con los cambios de temperatura, en caso de tormenta eléctrica un rayo, en caso de vendaval afectaciones a la infraestructura	Evento Natural
AM-06	Desastre natural	Cambios naturales que tienen un impacto devastador en las personas y las infraestructuras. Las causas de un desastre natural pueden ser fenómenos sísmicos, climáticos o volcánicos como terremotos, inundaciones, deslizamientos de tierra, tsunamis, avalanchas y erupciones volcánicas. Ejemplos de fenómenos meteorológicos extremos son tormentas eléctricas, huracanes o ciclones. Dependiendo de su ubicación, la institución está expuesta a estos riesgos derivados de varios tipos de desastres naturales en mayor o menor grado.	Evento Natural
AM-07	Obstaculización de la disponibilidad del personal	Los grandes eventos de todo tipo pueden impedir el funcionamiento adecuado de un organismo público o una empresa. Incluyen entre otras cosas festivales callejeros, conciertos, eventos deportivos, acción industrial o manifestaciones. Los disturbios relacionados con tales eventos pueden tener consecuencias adicionales, como la intimidación de los empleados hasta el uso de la fuerza contra el personal o el edificio.	Compromiso de funciones
AM-08	Pérdida del suministro de energía eléctrica	A pesar de la alta disponibilidad del suministro de energía en Bogotá. La mayoría de estas interrupciones son tan cortas, con tiempos de menos de un segundo. Pero las interrupciones de más de incluso 10 milisegundos son capaces de interrumpir la operación de TI. Sin embargo, además de las interrupciones en las redes de suministro, también los apagones causados por trabajos no anunciados o daños en los cables debido a trabajos de ingeniería civil pueden provocar fallas de energía. Muchas instalaciones de infraestructura dependen de la energía eléctrica actual, ascensores, dispositivos de aire acondicionado, sistemas de alarma, puertas de seguridad, cierre automático de puertas, sistemas de rociadores e incluso el suministro de agua en los edificios depende de la energía debido a las bombas en los pisos superiores requeridas para producir presión. Además de las fallas, otras interrupciones de la fuente de alimentación también pueden afectar la operación. Los picos de voltaje pueden, por ejemplo,	Pérdida de servicios esenciales

Código	Nombre	Descripción	Tipo
		provocar un mal funcionamiento o incluso daños en el equipo eléctrico.	
AM-09	Falla o interrupción de los servicios de proveedores	La falta de continuidad en la prestación de un servicio por parte de un contratista puede ser crítico para el desarrollo de la operación como es el caso del soporte de las diferentes aplicaciones o el mantenimiento correctivo de equipos que pueden afectar la disponibilidad de la información.	Compromiso de funciones
AM-10	Falla en el suministro de agua	Una falla o interrupción en el suministro de agua, puede conducir a una situación en la que, entre otras cosas, las personas ya no pueden trabajar en el edificio o en la operación de TI y, por lo tanto, el procesamiento de la información se ve afectado.	Pérdida de servicios esenciales
AM-11	Falla del sistema de aire acondicionado	La falla de los sistemas de refrigeración, ventilación y/o aire acondicionado, pueden generar temperaturas adversas tanto para personal y equipos, lo que puede ocasionar que las personas ya no pueden trabajar en el edificio o en la operación de TI o que los equipos operen en condiciones que puedan producir daños en los mismos.	Pérdida de servicios esenciales
AM-12	Falla de los equipos de Telecomunicaciones	Las conexiones de comunicación tales como teléfono, correo electrónico u otros servicios que utilizan redes de comunicaciones son esenciales, si alguna de estas no está disponible el resultado puede ser, por ejemplo, interrupción de actividades por falta de acceso a la información, limitando también la comunicación con los usuarios. Si las aplicaciones de tiempo crítico se ejecutan en sistemas de TI que están conectados a través de redes, puede presentar posibles pérdidas y daños consecuentes debido a una falla de la red. Pueden surgir problemas similares si las redes de comunicaciones requeridas se alteran, aunque no hayan fallado por completo. Los enlaces de comunicación pueden mostrar mayores tasas de error u otras deficiencias de calidad.	Pérdida de servicios esenciales

Código	Nombre	Descripción	Tipo
AM-13	Interceptación de información - Espionaje	El espionaje se define como ataques dirigidos a recopilar, evaluar y presentar información sobre empresas, personas, productos u objetivo. La información presentada se puede utilizar, por ejemplo, para proporcionar ciertas ventajas competitivas en procesos de contratación o suplantar o chantajear a las personas. Además de una variedad de ataques técnicamente complejos, a menudo también hay métodos mucho más simples para obtener información valiosa, por ejemplo, al reunir información de varias fuentes de acceso público, que parece información inofensiva aisladamente, pero puede ser comprometedora en otros contextos, dado que los datos confidenciales con frecuencia no están suficientemente protegidos.	Compromiso de Información
AM-14	Espionaje por interceptaciones tecnológicas	Los ataques dirigidos a conexiones de comunicación, conversaciones, fuentes de ruido de todo tipo o sistemas de TI con el objetivo de recopilar información se conocen como interceptaciones tecnológicas. Va desde espionaje clandestino y desapercibido en una conversación hasta ataques complejos altamente especializados para interceptar señales transmitidas por radio o líneas de transmisión, con la ayuda de antenas o sensores. Particularmente crítico es la transmisión desprotegida de datos de autenticación en protocolos de texto plano como HTTP, FTP o telnet, ya que pueden analizarse fácilmente de forma automática debido a la estructura clara de los datos.	Compromiso de Información
AM-15	Robo o pérdida de medios, equipos o documentos.	El robo de medios de almacenamiento de datos, sistemas de TI, accesorios, software o datos, por un lado, genera costos para el reemplazo y la restauración del estado operativo. Por otro lado, hay pérdidas debido a la falta de disponibilidad. Si se divulga información confidencial debido al robo, esto puede ocasionar daños adicionales. Además de los servidores y otros costosos sistemas de TI, también se roban con frecuencia los sistemas de TI móviles, que se transportan de manera discreta y fácil. Sin embargo, también los dispositivos de almacenamiento externo pueden se robados para acceder a su información.	Compromiso de Información
AM-16	Recuperación de información de medios reciclados o descartados	Al momento de descartar equipos o medios, se deben tomar las medidas que impidan que, de la manipulación de estos elementos, se pueda reconstruir o acceder a información confidencial. De los dispositivos y medios de almacenamiento puede recuperar información con técnicas y equipos especializados.	Compromiso de Información

Código	Nombre	Descripción	Tipo
AM-17	Mala planeación o falta de adaptación	Si los procesos organizativos que sirven al procesamiento de información directo o indirecto no están diseñados adecuadamente, puede provocar problemas de seguridad. Aunque cada paso del proceso se lleva a cabo correctamente, el daño a menudo ocurre porque los procesos se definen de manera incorrecta. Otra posible razón para los problemas de seguridad es la dependencia de otros procesos que no tienen ninguna relación aparente con el procesamiento de la información. Tales dependencias pueden ser fácilmente ignoradas durante la planificación y desencadenar impedimentos durante la operación. Además, pueden surgir problemas de seguridad cuando las tareas, roles o responsabilidades no están claramente asignados. Esto puede causar, entre otras cosas, retrasar los procesos, descuidar los procedimientos de seguridad o ignorar las regulaciones. Un peligro surge cuando los equipos, productos, procedimientos u otros medios para la implementación del procesamiento de la información no se implementan adecuadamente. La elección de productos inadecuados o puntos débiles en la arquitectura de la aplicación o en el diseño de la red, por ejemplo, puede generar problemas de seguridad.	Compromiso de funciones
AM-18	Divulgación de información confidencial	Los datos e información confidenciales solo deben ser accesibles para las personas que tienen autorizado el acceso a la información. Además de la integridad y la disponibilidad, la confidencialidad pertenece a los parámetros básicos de seguridad de la información. Para la información confidencial (como contraseñas, datos personales, secretos comerciales u oficiales, datos de desarrollo) existe el peligro inherente de que estos sean revelados por fallas técnicas, descuidos o también por acciones deliberadas.	Compromiso de Información
AM-19	Datos de fuentes no confiables	Si se utiliza información, software o equipos que provienen de fuentes poco confiables o cuyo origen y corrección no se verificaron suficientemente, su implementación puede presentar riesgos elevados. Puede llevar a que la información relevante del negocio descanse en la base de datos incorrecta, los cálculos que proporcionen resultados incorrectos o se tomen decisiones incorrectas, entre otras cosas. Además, la integridad de los sistemas de TI puede verse afectada por ello.	Compromiso de Información

Código	Nombre	Descripción	Tipo
AM-20	Manipulación de hardware o software	La manipulación se define como cualquier forma de intervención dirigida pero secreta con el objetivo de realizar cambios de manera inadvertida. La manipulación de hardware o software se puede realizar para generar daño deliberadamente, para obtener ventajas o ganancias personales. Puede centrarse en todo tipo de dispositivos, accesorios, medios de almacenamiento de datos, aplicaciones y bases de datos o similares. La manipulación de hardware y software no siempre conduce a una pérdida directa. Sin embargo, si dicha información procesada se ve afectada, esto puede conducir a todo tipo de implicaciones de seguridad (pérdida de confidencialidad, integridad o disponibilidad). De este modo, las manipulaciones pueden ser más efectivas cuanto más tarde se descubran, más amplio es el conocimiento que tienen los perpetradores y cuán más profundos serán los efectos en un proceso de trabajo. Los efectos van desde la inspección no autorizada de datos confidenciales hasta la destrucción de medios de almacenamiento de datos o TI	Compromiso de Información
AM-21	Manipulación de información	La información puede ser manipulada de varias maneras, mediante el registro incorrecto o intencionalmente falso de datos, cualquier cambio en el contenido de los campos de la base de datos o por correspondencia. En principio, esto no solo concierne a la información digital, sino también a los documentos en papel. Sin embargo, solo se puede manipular la información a la que tiene acceso. Cuantos más derechos de acceso a los archivos y directorios de los sistemas informáticos tenga una persona o más posibilidades de acceder a la información que tiene. Los documentos archivados generalmente contienen información confidencial. La manipulación de dichos documentos es particularmente grave porque, bajo ciertas circunstancias, pueden pasar años antes de que se note la manipulación y la verificación ya no será posible.	Compromiso de Información
AM-22	Acceso no Autorizado a sistemas informáticos	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno o por personas ajenas a la entidad.	Acciones no autorizadas

Código	Nombre	Descripción	Tipo
AM-23	Destrucción de dispositivos o medios de almacenamiento	La destrucción de los medios de almacenamiento de datos o los sistemas de TI puede dar lugar a tiempos de inactividad importantes para los procesos de la entidad. Debido a negligencia, uso indebido y también por manejo no capacitado, puede ocurrir la destrucción de dispositivos y medios de almacenamiento de datos, lo que perjudica seriamente el funcionamiento de los sistemas de TI. También existe el riesgo de que, junto con la destrucción, se pierda información importante, que no se puede reconstruir en absoluto o solo con gran esfuerzo.	Acciones no autorizadas
AM-24	Falla de dispositivos o sistemas	La falla de un solo componente de un sistema de TI puede conducir a una falla de toda la operación de TI y, por lo tanto, a la falla de los procesos críticos. En particular, los componentes clave de un sistema de TI, por ejemplo, servidores y elementos de acoplamiento de red, pueden causar tales fallas. Si las aplicaciones de tiempo crítico se ejecutan en un sistema de TI sin ninguna alternativa, los daños consecuentes después de una interrupción del sistema son respectivamente altos. Es importante detectar las fallas en los equipos y componentes con redundancia ya que pueden fallar y no ser detectados.	Falla técnica
AM-25	Mal funcionamiento de dispositivos o sistemas	Hay muchas causas de mal funcionamiento, como fatiga del material, tolerancias de fabricación, debilidades de diseño, límites excedidos, condiciones de uso no deseadas o falta de mantenimiento, por ejemplo. Como no hay dispositivos y sistemas perfectos, siempre se debe aceptar alguna probabilidad residual de mal funcionamiento. Un mal funcionamiento de un dispositivo o sistema puede afectar todos los parámetros básicos de seguridad de la información (confidencialidad, integridad, disponibilidad). Además, el mal funcionamiento puede pasar desapercibido bajo ciertas circunstancias por un período más largo.	Falla técnica
AM-26	Falta de recursos	Si los recursos disponibles en un área dada son insuficientes, pueden ocurrir fallas en el suministro atendido por estos recursos. La falta de recursos puede ocurrir en los procedimientos de gestión TIC, pero también en otras áreas de la entidad. Esto puede conducir a una variedad de efectos negativos si no se dispone de personal, tiempo y recursos financieros suficientes. La falta de implementación de controles puede afectar en el impacto o la frecuencia del riesgo.	Compromiso de funciones
AM-27	Violación de leyes o regulaciones	Si la información, los procesos misionales y los sistemas de TI de la entidad no están suficientemente protegidos, esto puede conducir a violaciones de las leyes relacionadas con el tratamiento de información o de los contratos existentes.	Compromiso de funciones

Código	Nombre	Descripción	Tipo
		Las leyes que deben incluirse son la de protección de datos personales	
AM-28	Error de uso o administración incorrecta de dispositivos y sistemas	El uso incorrecto o inadecuado de dispositivos, sistemas y aplicaciones puede afectar su seguridad, especialmente cuando se ignoran o se eluden las medidas de seguridad existentes. Esto a menudo conduce a interrupciones o fallas, también se puede violar la confidencialidad y la integridad de la información. Por ejemplo, los derechos de acceso demasiado generosos, las contraseñas fáciles de adivinar, los medios de almacenamiento de datos protegidos inadecuadamente que contienen copias de seguridad o terminales que no se bloquean durante una ausencia temporal pueden provocar incidentes de seguridad. Del mismo modo, los datos también se pueden eliminar o cambiar accidentalmente debido al uso incorrecto de los sistemas o aplicaciones de TI. Por lo tanto, la información confidencial puede estar disponible al público si, por ejemplo, los permisos se configuran incorrectamente. Si los cables de alimentación o de red se colocan sin protección, pueden dañarse inadvertidamente, lo que puede provocar una interrupción. Se puede desconectar una conexión de cable cuando el personal o los visitantes tropiezan con ella y es difícil de ubicar si no se encuentra debidamente rotulada.	Compromiso de funciones
AM-29	Abuso de derechos o autorizaciones	Dependiendo de sus roles y actividades a los usuarios se les otorgan los derechos de acceso correspondientes. De esta forma, el acceso a la información se controla y supervisa, para el desempeño de actividades de los usuarios. Definir niveles de acceso y permisos para el uso de sistemas de información. Se produce un mal uso de los privilegios cuando los permisos obtenidos de manera intencional, legal o ilegal se usan fuera del alcance del uso previsto. Los usuarios administrativos pueden generar riesgos de mayor impacto debido al nivel de privilegios para la gestión de la información.	Compromiso de funciones

Código	Nombre	Descripción	Tipo
AM-30	Ataque	Un ataque puede constituir una amenaza para una institución. Las posibilidades técnicas para perpetrar un ataque son numerosas: lanzamiento de ladrillos, explosiones, uso de armas de fuego o incendio provocado. Si una institución está expuesta al peligro de un ataque y en qué medida depende no solo de la ubicación y el entorno del edificio, sino también de las actividades de la institución y del clima sociopolítico. Las empresas y organismos públicos que operan en áreas políticamente controvertidas están más en riesgo que otros. Las instituciones cercanas a las áreas de demostración habituales están en mayor riesgo que aquellas en ubicaciones remotas. Para evaluar el nivel de amenaza o al sospechar la amenaza de ataques políticamente motivados, se puede consultar a las autoridades de investigación criminal. En el caso de los archivos, la evaluación de amenazas debe tener en cuenta una circunstancia especial: almacenan una gran cantidad de documentos y datos en un espacio relativamente pequeño. Su destrucción puede tener implicaciones de largo alcance, no solo para el archivo, sino también para otros usuarios. Por ejemplo, puede ser necesario en tal caso, que los datos perdidos se deban volver a recopilar o volver a registrar con gran esfuerzo. En ciertas circunstancias, algunos datos incluso se perderán irrevocablemente.	Acciones no autorizadas
AM-31	Coerción, Extorsión o Corrupción	La coerción, la extorsión o la corrupción pueden afectar la seguridad de la información y los procesos de la entidad. Usando amenazas de violencia u otros perjuicios, un atacante puede, tratar de hacer que la víctima no tenga en cuenta las pautas de seguridad o eludir las medidas de seguridad (coerción). En lugar de amenazar, los atacantes también pueden ofrecer a propósito dinero de los empleados u otras personas u otros beneficios para convertirlos en un instrumento para las violaciones de seguridad (corrupción). Existe el riesgo de que un empleado corrupto envíe documentos confidenciales a personas no autorizadas. En principio, por coerción o corrupción, todos los parámetros básicos de seguridad de la información pueden verse afectados.	Compromiso de funciones
AM-32	Suplantación	En caso de suplantación, un atacante asume una identidad falsa, aprovecha la información sobre otra persona para actuar en su nombre. Aquí, los datos como la fecha de nacimiento, dirección, tarjeta de crédito o números de cuenta bancaria se utilizan para acceder a un proveedor de Internet u obtener beneficios financieros de otras maneras. La suplantación a menudo conduce directa o indirectamente al daño de la reputación. Algunas formas de fraude de identidad también se conocen como disfraces. La suplantación ocurre con mayor frecuencia cuando la verificación de identidad se maneja de manera descuidada.	Compromiso de Información

Código	Nombre	Descripción	Tipo
AM-33	Repudio de acciones	Las personas pueden negar, por diversas razones, haber cometido ciertos actos, porque estos actos violan instrucciones, pautas de seguridad o incluso leyes. Pero también podrían negar haber recibido una notificación porque han olvidado una fecha límite o una cita. El campo de la seguridad de la información se centra en la responsabilidad, una propiedad predestinada para garantizar que los actos cometidos no se puedan negar sin justificación. En una comunicación hay una distinción adicional, si un participante de la comunicación niega la recepción de mensajes (Repudio de recibo) o el envío de mensajes (Repudio de origen). Rechazar la recepción de mensajes puede ser relevante para, entre otras cosas, transacciones financieras cuando alguien niega haber recibido una factura en la fecha de vencimiento. Del mismo modo, puede suceder que un participante de comunicación niegue el envío de mensajes.	Compromiso de funciones
AM-34	Distribución de software malicioso	El software malicioso es un software desarrollado con el objetivo de realizar operaciones no deseadas y a menudo perjudiciales. Los tipos típicos de software malicioso incluyen virus, gusanos, troyanos y malware. El software malicioso generalmente actúa de manera secreta sin el conocimiento o consentimiento del usuario. Hoy en día, el software malicioso ofrece a un atacante posibilidades integrales de comunicación y control, y pone a disposición una variedad de funciones. Entre otras cosas, el software malicioso puede revelar a propósito contraseñas, sistemas de control remoto, desactivar el software de protección de datos y espiar datos. El daño más significativo aquí es la pérdida o corrupción de información o aplicaciones. Pero también la pérdida de reputación y daños financieros, causados por software malicioso, son de gran importancia.	Compromiso de funciones

Código	Nombre	Descripción	Tipo
AM-35	Ataque de denegación de servicios	Hay una variedad de diferentes formas de ataque, todas con el objetivo de interrumpir el uso previsto de ciertos servicios, funciones o dispositivos. El término genérico para tales ataques es "Denegación de servicio". A menudo se usa el término "ataque DoS". Tales ataques pueden provenir, entre otros, de empleados o clientes descontentos, pero también de competidores, extorsionistas o perpetradores con motivaciones políticas. El objetivo de los ataques puede ser valores relevantes para la empresa de cualquier tipo. Las formas típicas de ataques DoS son: –Interrupciones de los procesos comerciales, por ejemplo, al inundar el procesamiento de pedidos con pedidos incorrectos, –Daño a la infraestructura, por ejemplo, bloqueando las puertas de la institución, –Provocando fallas de TI por e. sol. servicios de sobrecarga intencionados de un servidor en la red. Este tipo de ataque a menudo se asocia con recursos distribuidos, el atacante genera una demanda tan alta de estos recursos que ya no están disponibles para los usuarios reales. En los ataques basados en TI, los siguientes recursos pueden hacerse artificialmente escasos: procesos, tiempo de CPU, memoria, espacio en disco y capacidad de transferencia.	Falla técnica
AM-36	Sabotaje	El sabotaje es la manipulación o daño deliberado de objetos o procesos con el objetivo de infligir daño a la víctima actuando de esta manera. Los objetivos particularmente atractivos pueden ser los centros de datos y las conexiones de comunicación de entidades y organismos públicos, ya que se puede lograr un gran efecto con relativamente pocos recursos. La compleja infraestructura de un centro de datos puede verse afectada por la manipulación selectiva, cuando influyan activamente en componentes importantes para provocar interrupciones operativas. En este sentido, los sistemas de construcción técnica y la infraestructura de comunicación insuficientemente protegidos, así como los puntos centrales de suministro, están particularmente amenazados si no se observan en términos organizativos y técnicos, los externos pueden acceder fácilmente.	Compromiso de funciones

Código	Nombre	Descripción	Tipo
AM-37	Ingeniería Social	La ingeniería social es un método para obtener acceso no autorizado a información o sistemas de TI. En la ingeniería social se aprovechan las cualidades humanas tales como la amabilidad, confianza, miedo o respeto por la autoridad. Como resultado, los empleados pueden ser manipulados para que actúen de manera inadmisible. Otra estrategia para la ingeniería social sistemática es desarrollar una relación más larga con la víctima. Sin importancia, pero numerosas llamadas telefónicas por adelantado sirven al atacante para obtener conocimiento y aumentar la confianza de que puede utilizarlo más adelante. Muchos usuarios saben que no deben revelar sus contraseñas a nadie. Los ingenieros sociales lo saben y, por lo tanto, deben alcanzar el objetivo deseado utilizando otras formas.	Compromiso de funciones

9. Identificación de Vulnerabilidades

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

- Hardware
- Red
- Software
- Persona
- Organizacional
- Instalaciones
- Información

La vulnerabilidad por sí misma no implica la materialización del riesgo ya que debe ser explotada por una amenaza, las vulnerabilidades se codifican con las letras “VULN” y el número consecutivo de la vulnerabilidad. A continuación, se relacionan las 66 vulnerabilidades más comunes asociadas a los tipos de activos enunciados en el párrafo precedente.

Código	Vulnerabilidad	Tipo de Activo
VULN-01	Arquitectura de red insegura	Componente de Red
VULN-02	Colocación o instalación de cables eléctricos sin protección	Componente de Red
VULN-03	Conexiones de red pública sin protección	Componente de Red
VULN-04	Falta de control en datos de entrada y salida y emisor y receptor	Componente de Red
VULN-05	Inadecuada gestión de redes	Componente de Red
VULN-06	Mala gestión de contraseñas	Componente de Red
VULN-07	Punto único de fallas	Componente de Red

VULN-08	Redes accesibles a personas no autorizadas	Componente de Red
VULN-09	Sobre dependencia en un dispositivo o sistema	Componente de Red
VULN-10	Trafico sensible desprotegido	Componente de Red
VULN-11	Almacenamiento desprotegido	Hardware
VULN-12	Falta de cuidado en la disposición	Hardware
VULN-13	Falta de esquemas de reemplazo periódico	Hardware

Código	Vulnerabilidad	Tipo de Activo
VULN-14	Inadecuado control de cambios	Hardware
VULN-15	Mantenimiento inadecuado o instalación defectuosa de medios de almacenamiento	Hardware
VULN-16	Sistemas desprotegidos ante acceso no autorizado	Hardware
VULN-17	Susceptibilidad del equipamiento a alteraciones en el voltaje	Hardware
VULN-18	Susceptibilidad del equipamiento a la humedad, contaminación, polvo, corrosión o congelamiento	Hardware
VULN-19	Susceptibilidad del equipamiento a la temperatura	Hardware
VULN-20	Susceptibilidad del equipamiento a la radiación electromagnética	Hardware
VULN-21	Uso de equipamiento obsoleto	Hardware
VULN-22	Copiado sin control	Información
VULN-23	Nivel de confidencialidad no definido con claridad	Información
VULN-24	Reglas para control de acceso no definidos con claridad	Información
VULN-25	Única copia, sólo una copia de la información	Información
VULN-26	Acceso no restringido a instalaciones	Información
VULN-27	Falta de protección física del edificio, puertas y ventanas.	Instalaciones
VULN-28	Ubicación susceptible a desastres naturales	Instalaciones
VULN-29	Ubicación susceptible a pérdidas de agua	Instalaciones
VULN-30	Falta de auditorías regulares (supervisión)	Organizacional
VULN-31	Falta de informes de fallas registradas en los registros de administrador y operador	Organizacional
VULN-32	Falta de procedimientos de identificación y evaluación de riesgos	Organizacional
VULN-33	Falta de un proceso formal para la autorización de la información pública disponible.	Organizacional
VULN-34	Falta o disposiciones insuficientes (relativas a la seguridad) en los contratos con clientes y / o terceros	Organizacional
VULN-35	Acceso no restringido a instalaciones	Persona
VULN-36	Ausencia de personal	Persona
VULN-37	Empleados desmotivados o inconformes	Persona

VULN-38	Falta de un proceso formal para la revisión del derecho de acceso (supervisión)	Persona
VULN-39	Falta de mecanismos de monitoreo	Persona
VULN-40	Inadecuada supervisión de proveedores externos	Persona
VULN-41	Inadecuada supervisión del trabajo de los empleados	Persona
Código	**Vulnerabilidad**	**Tipo de Activo**
VULN-42	Inadecuado nivel de conocimiento y/o concienciación de empleados	Persona
VULN-43	Procedimientos inadecuados de reclutamiento	Persona
VULN-44	Reglas organizacionales no definidas con claridad	Persona
VULN-45	Bases de datos con protección desactualizada contra códigos maliciosos	Software
VULN-46	Contraseñas inseguras	Software
VULN-47	Defectos bien conocidos en el software	Software
VULN-48	Descarga y uso incontrolado de software	Software
VULN-49	Eliminación de soportes de almacenamiento sin borrado de datos	Software
VULN-50	Falta de copias de respaldo	Software
VULN-51	Falta de mecanismos de identificación y autenticación	Software
VULN-52	Falta de separación de entornos de prueba y operativos	Software
VULN-53	Inadecuada o falta de implementación de auditoría interna	Software
VULN-54	Inadecuado control de cambios	Software
VULN-55	Inadecuados derechos de usuario	Software
VULN-56	Incorrecta configuración de parámetros	Software
VULN-57	Interfaz de usuario complicada	Software
VULN-58	Mala gestión de contraseñas	Software
VULN-59	Nulo o insuficiente protocolo de prueba de software	Software
VULN-60	Poderes de gran alcance	Software
VULN-61	Requisitos para desarrollo de software no definidos con claridad	Software
VULN-62	Sesiones activas después del horario laboral o al dejar la estación de trabajo	Software
VULN-63	Software inmaduro o nuevo	Software
VULN-64	Software no documentado	Software
VULN-65	Tablas de contraseña desprotegidas	Software
VULN-66	Uso no controlado de sistemas de información	Software

10. Identificación de Riesgos:

Una vez identificadas las amenazas y vulnerabilidades se deben identificar los riesgos

basados en los activos de la información. Para ello se ha elaborado una tabla que permite la identificación general del riesgo relacionando con el tipo de activo de información, asociando la vulnerabilidad por explotar, la amenaza y la consecuencia del riesgo.

IDENTIFICACIÓN DE LOS RIESGOS Y CONSECUENCIAS

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
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 personas
Hardware	Pérdida de la Disponibilidad	Almacenamiento desprotegido	Robo de medios, equipos o documentos.	Posibilidad de pérdida de acceso a información que no esté respaldada	No disponibilidad de información
Hardware	Pérdida de la Integridad	Almacenamiento desprotegido	Manipulación de información	Modificación de la información.	Publicación de información que no es cierta, responder a la ciudadanía de manera inadecuada
Hardware	Pérdida de la Confidencialidad	Falta de cuidado en la disposición	Recuperación de información de medios reciclados o descartados	Que una persona sin autorización de acceso a la información pueda tenerla por falta de cuidado en su disposición.	Uso inadecuado de la información.
Hardware	Pérdida de la Integridad	Falta de esquemas de reemplazo periódico	Mal funcionamiento de dispositivos o sistemas	Falta de redundancias en los equipos y sus componentes.	Que la información no se almacene de manera adecuada y quede desactualizada

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Hardware	Pérdida de la Disponibilidad	Falta de esquemas de reemplazo periódico	Mal funcionamiento de dispositivos o sistemas	Falta de redundancias en los equipos y sus componentes.	Pérdida de la información o el acceso a ella.
Hardware	Pérdida de la Disponibilidad	Mantenimiento inadecuado o instalación defectuosa de medios de almacenamiento	Mal funcionamiento de dispositivos o sistemas	Posibilidad de falla en los dispositivos que integran la infraestructura de la entidad	No disponibilidad de la información servicios de TI
Hardware	Pérdida de la Confidencialidad	Inadecuado control de cambios	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Posibilidad de administración inadecuada de los dispositivos	Riesgo de versiones que permitan acceder a personas sin autorización a la información
Hardware	Pérdida de la Integridad	Inadecuado control de cambios	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Publicar versiones desactualizadas	Que se presenten o se publiquen versiones desactualizadas de los documentos
Hardware	Pérdida de la Disponibilidad	Inadecuado control de cambios	Error de uso, uso o administración incorrectos de dispositivos y sistemas	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.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Hardware	Pérdida de la Disponibilidad	Mantenimiento inadecuado o instalación defectuosa de medios de almacenamiento	Destrucción de dispositivos o de medios 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.
Hardware	Pérdida de la Integridad	Sistemas desprotegidos ante acceso no autorizado	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 autorización.
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.	Alteración de la información institucional sin autorización.
Hardware	Pérdida de la Confidencialidad	Sistemas desprotegidos ante acceso no autorizado	Acceso no autorizado a sistemas informáticos	No tener herramientas de verificación de acceso	Acceso de personas no autorizadas a información clasificada o reservada.
Hardware	Pérdida de la Integridad	Sistemas desprotegidos ante acceso no autorizado	Acceso no autorizado a sistemas informáticos	No tener herramientas de verificación de acceso	Alteración de la información institucional sin autorización.
Hardware	Pérdida de la Disponibilidad	Sistemas desprotegidos ante acceso no autorizado	Acceso no autorizado a sistemas informáticos	No tener herramientas de verificación de acceso	Eliminación de información por parte de usuarios no autorizados

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
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	Pérdida de la Disponibilidad	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
Hardware	Pérdida de la Disponibilidad	Susceptibilidad del equipamiento a la temperatura	Fenómenos climáticos y meteorológicos	Afectación a los equipos de procesamiento falla del aire acondicionado por dimensionamiento.	Pérdida de accesos a la información por falla en los equipos
Hardware	Pérdida de la Disponibilidad	Susceptibilidad del equipamiento 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.	Pérdida de accesos a la información 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.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Red	Pérdida de la Integridad	Arquitectura de red insegura	Mala planeación o falta de adaptación	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.
Red	Pérdida de la Disponibilidad	Arquitectura de red insegura	Mala planeación o falta de adaptación	Acceso de personas no autorizadas a los sistemas de información de la entidad. Que puedan eliminar la información.	Eliminación de información institucional, que pueda llegar a tener consecuencias legales.
Red	Pérdida de la Confidencialidad	Conexiones de red pública sin protección	Acceso no autorizado a sistemas informáticos	Falta de aplicación reglas de administración, que brinden seguridad a la red.	Acceso de personas no autorizadas a información clasificada o reservada.
Red	Pérdida de la Integridad	Conexiones de red pública sin protección	Acceso no autorizado a sistemas informáticos	Falta de aplicación reglas de administración, que brinden seguridad a la red.	Alteraciones en la información debido al acceso de personas no autorizadas a información clasificada o reservada.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Red	Pérdida de la Disponibilidad	Conexiones de red pública sin protección	Acceso no autorizado a sistemas informáticos	Falta de aplicación de reglas de administración, que brinden seguridad a la red.	Eliminación de información debido al acceso de personas no autorizadas a información clasificada o reservada.
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
Red	Pérdida de la Integridad	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.	Alteración de información clasificada o reservada por personas no autorizadas
Red	Pérdida de la Disponibilidad	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.	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 dispositivos y sistemas	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.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Red	Pérdida de la Disponibilidad	Inadecuada gestión de redes	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Acceso no autorizado a los sistemas de información de la entidad.	Eliminación de información.
Red	Pérdida de la Confidencialidad	Mala gestión de contraseñas	Robo de identidad	Accesos a sistemas de información a personas no autorizadas	Divulgación de información de manera inadecuada, suplantación
Red	Pérdida de la Integridad	Mala gestión de contraseñas	Robo de identidad	Accesos a sistemas de información a personas no autorizadas	Divulgación de información de manera inadecuada, suplantación
Red	Pérdida de la Disponibilidad	Mala gestión de contraseñas	Robo de identidad	Accesos a sistemas de información a personas no autorizadas	Eliminación de información, que puede traer consecuencias legales.
Red	Pérdida de la Integridad	Punto único de fallas	Falla de los equipos de Telecomunicaciones	Presentar fallas en equipos de telecomunicaciones centralizados en un punto único y no tener redundancia	Información alterada o desincronizada
Red	Pérdida de la Disponibilidad	Punto único de fallas	Falla de los equipos de Telecomunicaciones	Presentar fallas en equipos de telecom centralizados en un punto único y no tener redundanciaunicaciones	No tener disponibilidad de los canales de comunicación de la entidad y que afecte su misionalidad.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Red	Pérdida de la Confidencialidad	Redes accesibles a personas no autorizadas	Robo de identidad	Suplantación de usuario.	Suplantación para uso indebido de la información.
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 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 autorizados debido a los defectos o fallas de los sistemas	Alteraciones en la información, problemas para el acceso y disponibilidad de la información.
Software	Pérdida de la Integridad	Defectos bien conocidos en el software	Mal funcionamiento 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 autorizados debido a los defectos o fallas de los sistemas	Alteraciones en la información, problemas para el acceso y disponibilidad de la información.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Disponibilidad	Defectos bien conocidos en el software	Mal funcionamiento 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 autorizados debido a los defectos o fallas de los sistemas	Alteraciones en la información, problemas para el acceso y disponibilidad de la información.
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.
Software	Pérdida de la Integridad	Bases de datos con protección desactualizada contra códigos maliciosos	Distribución de software malicioso	Aparición de nuevos códigos maliciosos que afecten los sistemas de información	Alteración u ocultamiento de información de la entidad.
Software	Pérdida de la Confidencialidad / Integridad / Disponibilidad	Contraseñas inseguras	Acceso no autorizado a sistemas informáticos	Posibilidad de acceso no autorizado a los sistemas de información y documentos electrónicos	Exposición de información clasificada o reservada de la entidad

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Confidencialidad	Defectos bien conocidos en el software	Espionaje por interceptaciones tecnológicas		
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 clasificada o reservada de la entidad
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 información confidencial.
Software	Pérdida de la Integridad	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.	Alteración de los sistemas de información.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Disponibilidad	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.	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.
Software	Pérdida de la Integridad	Descarga y uso incontrolado de software	Distribución de software malicioso	Uso de aplicaciones inseguras que afecten los sistemas de información	Alteración de los sistemas de información.
Software	Pérdida de la Disponibilidad	Descarga y uso incontrolado de software	Distribución de software malicioso	Uso de aplicaciones inseguras que afecten los sistemas de información	Eliminación o secuestro de información.
Software	Pérdida de la Confidencialidad	Eliminación de soportes de almacenamiento sin borrado de datos	Recuperación de información de medios reciclados o descartados	Extracción de información de medios de almacenamiento desechados.	Acceso a información reservada o clasificada a personal no autorizado.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Disponibilidad	Falta de copias de respaldo	Destrucción de dispositivos o medios de almacenamiento	Destrucción no autorizada de información no respaldada.	Pérdida definitiva de información de la entidad
Software	Pérdida de la Disponibilidad	Falta de copias de respaldo	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.
Software	Pérdida de la Integridad	Falta de mecanismos de identificación y autenticación	Repudio de acciones	Alteraciones en los sistemas de información sin verificación de identidad.	Modificaciones en la información sin identificación del 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.
Software	Pérdida de la Integridad	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	Modificación a la información sin identificación de usuario o con un usuario ajeno.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Disponibilidad	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	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.
Software	Pérdida de la Integridad	Falta de separación de entornos de prueba y operativos	Manipulación de hardware o software	Procesar y presentar información de prueba que no esté verificada.	Gestionar información sin garantías de procesamiento o modificar información de la entidad sin autorización.
Software	Pérdida de la Disponibilidad	Falta de separación de entornos de prueba y operativos	Manipulación de hardware o software	Información eliminada en realización de pruebas.	Eliminación de información oficial de la entidad sin autorización.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Confidencialidad	Inadecuada o falta de implementación de auditoría interna	Mala planeación o falta de adaptación	Falta de realización de las actividades programadas para la implementación de controles relacionados con el tratamiento de riesgo en seguridad y privacidad de la información.	Falta de verificación de accesos a los sistemas de información.
Software	Pérdida de la Integridad	Inadecuada o falta de implementación de auditoría interna	Mala planeación o falta de adaptación		Falta de verificación de la calidad de información de la entidad.
Software	Pérdida de la Disponibilidad	Inadecuada o falta de implementación de auditoría interna	Mala planeación o falta de adaptación	Falta de realización de las actividades programadas para la implementación de controles relacionados con el tratamiento de riesgo en seguridad y privacidad de la información.	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 sistemas	Uso de versiones desactualizadas de los sistemas de información, errores de configuración o generación de permisos.	Acceso de información a usuarios no autorizados o incognitos.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Integridad	Inadecuado control de cambios	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Uso de versiones desactualizadas de los sistemas de información, errores de configuración o generación de permisos.	Cambios en la información o en las condiciones de procesamiento
Software	Pérdida de la Disponibilidad	Inadecuado control de cambios	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Uso de versiones desactualizadas de los sistemas de información, errores de configuración o generación de permisos.	Cambios en la información o en las condiciones de procesamiento
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 autorizados.
Software	Pérdida de la Integridad	Inadecuados derechos de usuario	Abuso de derechos o autorizaciones	Usuarios administrativos o con altos privilegios que realicen cambios en accesos o configuraciones sin autorización	Modificaciones en la información o en sus registros sin autorización.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Disponibilidad	Inadecuados derechos de usuario	Abuso de derechos o autorizaciones	Usuarios administrativos o con altos privilegios que realicen cambios en accesos o configuraciones sin autorización	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 Integridad	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.
Software	Pérdida de la Disponibilidad	Incorrecta configuración de parámetros	Mal funcionamiento de dispositivos o sistemas	Error en la configuración de los parámetros de seguridad de los sistemas de información	Falta de acceso a la información en el momento requerido.
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	Personas no autorizadas con acceso a los sistemas de información.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Integridad	Interfaz de usuario complicada	Error de uso, uso o administración 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.
Software	Pérdida de la Disponibilidad	Interfaz de usuario complicada	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Falta de conocimiento de los usuarios en el manejo de los sistemas de información	Borrado de información por falta de manejo de las interfaces.
Software	Pérdida de la Confidencialidad	Interfaz de usuario complicada	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Falta de conocimiento de los usuarios en el manejo de los sistemas de información	Eliminación de información de manera involuntaria.
Software	Pérdida de la Integridad	Mala gestión de contraseñas	Robo de identidad	Personas que averigüen el usuario y contraseña de manera inescrupulosa	Uso inadecuado de los sistemas de información
Software	Pérdida de la Disponibilidad	Mala gestión de contraseñas	Robo de identidad	Eliminación de información de manera intencional por parte de un tercero.	Eliminación de información sin autorización y sin trazabilidad de usuario.
Software	Pérdida de la Confidencialidad	Mala gestión de contraseñas	Robo de identidad	Personas que averigüen el usuario y contraseña de manera inescrupulosa	Uso inadecuado de los sistemas de información

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Integridad	Requisitos para desarrollo de software no definidos con claridad	Mal funcionamiento de dispositivos o sistemas	Falta de conocimiento de la configuración del software.	Procesamiento de la información erróneo o equivocado
Software	Pérdida de la Disponibilidad	Requisitos para desarrollo de software no definidos con claridad	Mal funcionamiento de dispositivos o sistemas	Falta de conocimiento de la configuración del software.	Borrado de información
Software	Pérdida de la Confidencialidad	Requisitos para desarrollo de software no definidos con claridad	Mal funcionamiento de dispositivos o sistemas	Falta de conocimiento de la configuración del software.	Que existan salidas de información no autorizadas y que pueda llegar a personas no autorizadas.
Software	Pérdida de la Integridad / Disponibilidad y Confidencialidad.	Sesiones activas después del horario laboral o al dejar la estación de trabajo	Acceso no autorizado a sistemas informáticos	Posibilidad de exposición de información clasificada o reservada de manera remota o por atacantes	Exposición de información clasificada o reservada de la entidad
Software	Pérdida de la Integridad	Software inmaduro o nuevo	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Errores en procesamiento por fallas en la programación y en la configuración del sistema de información	Procesamiento de información errónea generando resultados equivocados.
Software	Pérdida de la disponibilidad	Software inmaduro o nuevo	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Errores en procesamiento por fallas en la programación y en la configuración del sistema de información	Borrado de información por error en el procesamiento de información y falta de acceso a los códigos fuente.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Confidencialidad	Software inmaduro o nuevo	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Errores en procesamiento por fallas en la programación y en la configuración del sistema de información	Acceso a terceros no autorizados a los sistemas de información
Software	Pérdida de la Integridad	Software inmaduro o nuevo	Mal funcionamiento de dispositivos o sistemas	Errores en procesamiento por fallas en el funcionamiento de los sistemas de información	Procesamiento de información errónea generando resultados equivocados.
Software	Pérdida de la Disponibilidad	Software inmaduro o nuevo	Mal funcionamiento de dispositivos o sistemas	Errores en procesamiento por fallas en el funcionamiento de los sistemas de información	Borrado de información por error en el procesamiento de información.
Software	Pérdida de la Confidencialidad	Software inmaduro o nuevo	Mal funcionamiento de dispositivos o sistemas	Errores en procesamiento por fallas en el funcionamiento de los sistemas de información	Acceso a terceros no autorizados a los sistemas de información
Software	Pérdida de la Integridad	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 procesamiento.	Modificaciones en los procesamientos de información sin identificar su causa

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Software	Pérdida de la Disponibilidad	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 procesamiento.	Borrado de información involuntario o falta de acceso a los sistemas de información a usuarios autorizados.
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 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 Integridad	Uso no controlado de sistemas de información.	Manipulación de información	Falta de control de los accesos a los sistemas de información	Usuarios no autorizados con acceso a la información

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Persona	Pérdida de la Integridad	Falta o disposiciones insuficientes (relativas a la seguridad) en los contratos 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.
Persona	Pérdida de la Disponibilidad	Falta o disposiciones insuficientes (relativas a la seguridad) en los contratos con clientes y / o terceros	Abuso de derechos o autorizaciones	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
Persona	Pérdida de la Confidencialidad	Falta o disposiciones insuficientes (relativas a la seguridad) en los contratos con clientes y / o terceros	Abuso de derechos o autorizaciones	Divulgación de información clasificada o reservada de la entidad	Materialización de riesgo legal en relación al tratamiento de datos personales.
Persona	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 reservada o clasificada.
Persona	Pérdida de la Disponibilidad	Acceso no restringido a instalaciones	Robo de medios, equipos o documentos.	Que personas no autorizadas tomen equipos, medios de almacenamiento o documentos.	No poder acceder a la información debido a la pérdida del archivo donde se encuentra almacenada.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Persona	Pérdida de la Disponibilidad	Ausencia de personal	Obstaculización de la disponibilidad del personal	Falta de personal con la información o falta de personal para responder a tiempo requerimientos de información	Falta de disponibilidad de información a la ciudadanía o a 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 clasificada y reservada.
Persona	Pérdida de la Disponibilidad	Empleados desmotivados o inconformes	Robo de medios, equipos o documentos.	Contratistas o servidores que lleven medios de almacenamiento, equipos o documentos sin autorización.	Falta de información por pérdida de equipos o documentos.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Persona	Pérdida de la Disponibilidad	Empleados desmotivados o inconformes	Sabotaje	Sabotaje a las condiciones de seguridad a los sistemas de información.	Eliminación o alteración de la información de manera voluntaria y no autorizada por parte de servidores 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.
Persona	Pérdida de la Disponibilidad	Empleados desmotivados o inconformes	Coerción, Extorsión o Corrupción	Eliminación de información de manera no autorizada.	Eliminación de información sin autorización o falta de acceso a los sistemas de información en momentos necesarios.
Persona	Pérdida de la Confidencialidad	Empleados desmotivados o inconformes	Coerción, Extorsión o Corrupción	Corrupción conocimiento de información de contratación en condiciones desiguales.	Desigualdad en la contratación de proveedores o contratistas.
Persona	Pérdida de la Integridad	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

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Persona	Pérdida de la Disponibilidad	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	Eliminación de información no autorizada por parte de usuarios no identificados, suplantación o usuarios que deberían estar inactivos.
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	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 autorizado.
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 debido a su robo.
Persona	Pérdida de la Disponibilidad	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	Falta de acceso a sistemas de información o a documentos debido a su robo.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
				usuarios a los sistemas de información.	
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.
Persona	Pérdida de la Integridad	Falta de mecanismos de monitoreo	Repudio de acciones	No aceptación de recepción o envío de comunicaciones.	Modificación en las comunicaciones que no garanticen el repudio.
Persona	Pérdida de la Integridad	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
Persona	Pérdida de la Disponibilidad	Inadecuada supervisión de proveedores externos	Abuso de derechos o autorizaciones	No revisar los accesos de los proveedores e identificar los puntos de acceso.	Eliminación de información sin autorización o falta de disponibilidad de los sistemas de información.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
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 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.
Persona	Pérdida de la Integridad	Inadecuado nivel de conocimiento y/o concienciación de servidores públicos	Ingeniería Social	Falta de conocimientos del personal de condiciones de seguridad de la información.	Modificaciones en los sistemas de información no autorizadas y con usuarios no propios.
Persona	Pérdida de la Integridad	Inadecuado nivel de conocimiento y/o concienciación de empleados	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Errores en el uso de sistemas de información.	Modificaciones en los sistemas de información no programadas o no autorizadas, debido a la falta de conocimiento en el manejo de los sistemas de información.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Persona	Pérdida de la Disponibilidad	Inadecuado nivel de conocimiento y/o concienciación de empleados	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Errores en el uso de sistemas de información.	Eliminación de información de manera involuntaria o restricción a los accesos de información de manera no autorizada
Persona	Pérdida de la Confidencialidad	Inadecuado nivel de conocimiento y/o concienciación de empleados	Error de uso, uso o administración incorrectos de dispositivos y sistemas	Errores en el uso de sistemas de información.	Uso de los sistemas de información por parte de personas no autorizadas o que no 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
Organizacional	Pérdida de la Disponibilidad	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.	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.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Organizacional	Pérdida de la Integridad	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.	Modificaciones de información de usuarios no autorizados.
Organizacional	Pérdida de la Disponibilidad	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.	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.	No publicar la información en los tiempos definidos por la entidad o por los entes de control.
Organizacional	Pérdida de la Integridad	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.	Publicar información que no haya sido revisada de manera previa.
Instalaciones	Pérdida de la Confidencialidad	Acceso no restringido a instalaciones	Robo de medios, equipos o documentos.	La falta de identificación y autorización de ingreso de visitantes	Personas no autorizadas con acceso a información.
Instalaciones	Pérdida de la Disponibilidad	Acceso no restringido a instalaciones	Robo de medios, equipos o documentos.	La falta de identificación y autorización de ingreso de visitantes	Perdida de información almacenada en medios externos o equipos que no pueda ser recuperada.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
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.
Instalaciones	Pérdida de la Integridad	Acceso no restringido a instalaciones	Manipulación de hardware o software	Visitantes que accedan a los equipos de la entidad sin autorización.	Modificaciones a la información sin autorización.
Instalaciones	Pérdida de la Disponibilidad	Acceso no restringido a instalaciones	Manipulación de hardware o software	Visitantes que accedan a los equipos de la entidad sin autorización.	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 Disponibilidad	Ausencia de personal	Desastre ambiental	Como el caso de la pandemia debido al COVID – 19 donde se tomaron medidas de restricción en la movilidad de las personas.	Falta de información a la ciudadanía o a los entes de control de forma oportuna.
Persona	Pérdida de la Disponibilidad	Ausencia de personal	Desastre natural	Presentación de un desastre natural que afecte la capacidad de asistencia de los servidores a las instalaciones de la entidad.	Falta de información a la ciudadanía o a los entes de control de forma oportuna.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Persona	Pérdida de la Disponibilidad	Ausencia de personal	Fenómenos climáticos y meteorológicos	Debido a factores climatológicos o meteorológicos los servidores de la entidad no puedan asistir a las instalaciones	Falta de información a la ciudadanía o a los entes de control de forma oportuna.
Información	Pérdida de la Confidencialidad	Copiado sin control	Divulgación de información confidencial	Dejar documentos en los centros de impresión y copiado	Personas no autorizadas pueden acceder a la información no custodiada.
Información	Pérdida de la Confidencialidad	Nivel de confidencialidad no definido con claridad	Divulgación de información confidencial	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.
Información	Pérdida de la Confidencialidad	Nivel de confidencialidad no definido con claridad	Violación de leyes o regulaciones	La falta de clasificación de la información no permitirá definir los controles necesarios para su seguridad.	Personas no autorizadas con acceso a la información clasificada y reservada.
Información	Pérdida de la Integridad	Nivel de confidencialidad no definido con claridad	Violación de leyes o regulaciones	La falta de clasificación de la información no permitirá definir los controles necesarios para su seguridad.	Modificaciones no autorizadas de información.
Información	Pérdida de la Disponibilidad	Nivel de confidencialidad no definido con claridad	Violación de leyes o regulaciones	La falta de clasificación de la información no permitirá definir los controles necesarios para su seguridad.	Eliminación de información sin autorización que pueda ser requerida por un organismo de control.

TIPO DE ACTIVO	RIESGO	VULNERABILIDADES / CAUSA	AMENAZA	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DEL RIESGO
Información	Pérdida de la Confidencialidad	Reglas para control de acceso no definidos con claridad	Abuso de derechos o autorizaciones	Personas con mayores accesos a la información que los autorizados	Acceso a información no autorizada.
Información	Pérdida de la Integridad	Reglas para control de acceso no definidos con claridad	Abuso de derechos o autorizaciones	Personas con mayores accesos a la información que los autorizados	Modificaciones no autorizadas a información a la cual no debería tener acceso el usuario
Información	Pérdida de la Disponibilidad	Reglas para control de acceso no definidos con claridad	Abuso de derechos o autorizaciones	Personas con mayores accesos a la información que los autorizados	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.

11. Evaluación del riesgo

El sistema de evaluación del riesgo está basado en dos variables, la probabilidad y el impacto.

Con relación a la probabilidad se establecieron los siguientes criterios para la evaluación:

CATEGORIA	PUNTAJE	DESCRIPCION
MUY IMPROBABLE	1	Riesgo cuya probabilidad de ocurrencia es MUY IMPROBABLE, es decir, se tiene entre un valor del 0% y del 10% de seguridad de que el riesgo se presente
IMPROBABLE	2	Riesgo cuya probabilidad de ocurrencia es IMPROBABLE, es decir, se tiene entre un valor mayor al 11% y un 30% de seguridad que el riesgo se presente

POSIBLE	3	Riesgo cuya probabilidad de ocurrencia es MODERADO, es decir, se tiene entre un valor mayor al 31% y un 65% de seguridad que el riesgo se presente
PROBABLE	4	Riesgo cuya probabilidad de ocurrencia es PROBABLE, es decir, se tiene entre un valor mayor al 66% y un 89% de seguridad que el riesgo se presente
CASI SEGURO	5	Riesgo cuya probabilidad de ocurrencia es CASI CIERTO, es decir, se tiene entre un valor mayor al 90% y un 100% de seguridad que el riesgo se presente

El siguiente criterio en la evaluación de riesgos es el impacto para lo cual se establecieron los siguientes criterios.

IMPACTO	ESCALA DE IMPACTO	CUANTITATIVO	CUALITATIVO
Insignificante	1	Insignificante Afectación ≥ 0.1% de los servicios que se prestan a la ciudadanía Afectación ≥ 0.5% del presupuesto anual de la Entidad	Sin afectación de la integridad. Sin afectación de la disponibilidad o una afectación leve Sin afectación de la confidencialidad.
Menor	2	Menor Afectación ≥ 0.5% de los servicios que se prestan a la ciudadanía Afectación ≥ 1% del presupuesto anual de la Entidad	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad. Afectación leve del medio ambiente

IMPACTO	ESCALA DE IMPACTO	CUANTITATIVO	CUALITATIVO
Moderado	3	Moderado Afectación ≥ 1.5% de los servicios que se prestan a la ciudadanía	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad. de la información debido al interés particular de los empleados y terceros. Afectación media del medio ambiente
Mayor	4	Mayor Afectación ≥ 2% de los servicios que se prestan a la ciudadanía Afectación ≥ 20% del presupuesto anual de la Entidad	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. Afectación alta del medio ambiente

IMPACTO	ESCALA DE IMPACTO	CUANTITATIVO	CUALITATIVO
Catastrófico	5	Catastrófico Afectación ≥ 5% de los servicios que se prestan a la ciudadanía Afectación ≥ 50% del presupuesto anual de la Entidad	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. Afectación alta del medio ambiente

La evaluación del riesgo es la multiplicación de los factores probabilidad e impacto, el resultado se clasifica en el mapa de calor el cual se presenta la siguiente tabla de valor.

Impacto	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		Probabilidad				

Con base en el resultado se planifica la posible acción frente al riesgo

RESULTADO DE EVALUACIÓN DEL RIESGO

		Cualitativo	Acciones
1	5	Bajo	Asumir
6	11	Moderado	Asumir y revisar
12	16	Alto	Reducir, evitar, compartir o transferir
17	25	Extremadamente alto	Reducir, evitar, compartir o transferir

PLAN DE TRATAMIENTO DE RIESGOS PARA LA UAECOB PARA EL 2026

PROCESO	GRUPO DE TRABAJO	ID	RIESGO	CAUSA	ACCIONES ASOCIADAS AL CONTROL	Fecha Inicio	Fecha Terminación	RESPONSABLE
GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	**R2**	PERDIDA DE CONFIDENCIALIDAD	SF29- Perdida de Confidencialidad de la información. Por fuga de información por deficiente gestión en la hardenizacion de componentes tecnológicos y definición de plantillas de seguridad (las provee el fabricante) para mantener configuraciones seguras en la línea base.	Establecer plantillas o listas de chequeo de aseguramiento de servidores en sus respectivos sistemas operativos. Compra de herramienta de remediación. / / / /	2/11/2024	14/11/2026	Tecnología. / / / /
- TODOS LOS PROCESOS	TODOS LOS PROCESOS	**R11**	PERDIDA DE CONFIDENCIALIDAD	PE10- Perdida de Confidencialidad, Integridad o Disponibilidad de la información. Incumplimiento de políticas de seguridad de la información por parte de funcionarios y terceros (proveedores, contratistas, outsourcing, otros).	Socialización de políticas de seguridad de la información. / / / /	14/11/2024	14/12/2026	Todos los procesos / / / /
TODOS LOS PROCESOS	TODOS LOS PROCESOS	**R14**	PERDIDA DE DISPONIBILIDAD	SF26- Indisponibilidad de la información. Por actos mal intencionados por Vulnerabilidad día cero a	Realizar gestión continua sobre buzones comprometidos / / / /	13/01/2026	26/03/2026	Mesa de Ayuda / / / /

PROCESO	GRUPO DE TRABAJO	ID	RIESGO	CAUSA	ACCIONES ASOCIADAS AL CONTROL	Fecha Inicio	Fecha Terminación	RESPONSABLE
				través de una variante de ransomware.				
GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	**R15**	PERDIDA DE CONFIDENCIALIDAD	SF26- Indisponibilidad de la información. Por actos mal intencionados por Vulnerabilidad día cero a través de una variante de ransomware.	Contramedidas requeridas para evitar la acción de aplicaciones Outh y usuarios comprometidos. / / / /	13/01/2026	10/02/2026	Grupo TIC / / / /
GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	**R16**	PERDIDA DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD	SF38- Perdida de Confidencialidad, Integridad y Disponibilidad de la Información por malware en plataforma de servidores por falta de gestión de vulnerabilidades y buenas prácticas de aseguramiento en sistemas operativos, bases de datos y/o aplicaciones.	Realizar gestión de vulnerabilidades técnicas sobre servidor. / / / /	13/01/2026	17/06/2026	Grupo TIC / / / /
GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	**R17**	PERDIDA DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD	SF38- Perdida de Confidencialidad, Integridad y Disponibilidad de la Información por malware en plataforma de servidores por falta de gestión de vulnerabilidades y buenas prácticas de	Realizar gestión de vulnerabilidades técnicas sobre servidor. / / / /	13/01/2026	17/06/2026	Grupo TIC / / / /

PROCESO	GRUPO DE TRABAJO	ID	RIESGO	CAUSA	ACCIONES ASOCIADAS AL CONTROL	Fecha Inicio	Fecha Terminación	RESPONSABLE
				aseguramiento en sistemas operativos, bases de datos y/o aplicaciones.				
GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	**R18**	PERDIDA DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD	SF38- Perdida de Confidencialidad, Integridad y Disponibilidad de la Información por malware en plataforma de servidores por falta de gestión de vulnerabilidades y buenas prácticas de aseguramiento en sistemas operativos, bases de datos y/o aplicaciones.	Realizar gestión de vulnerabilidades técnicas sobre servidor. / / / /	13/01/2026	17/06/2026	Grupo TIC / / / /
GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	**R19**	PERDIDA DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD	SF38- Perdida de Confidencialidad, Integridad y Disponibilidad de la Información por malware en plataforma de servidores por falta de gestión de vulnerabilidades y buenas prácticas de aseguramiento en sistemas operativos, bases de datos y/o aplicaciones.	Realizar gestión de vulnerabilidades técnicas sobre servidor. / / / /	13/01/2026	17/06/2026	Grupo TIC / / / /

PROCESO	GRUPO DE TRABAJO	ID	RIESGO	CAUSA	ACCIONES ASOCIADAS AL CONTROL	Fecha Inicio	Fecha Terminación	RESPONSABLE
GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	**R20**	PERDIDA DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD	SF38- Perdida de Confidencialidad, Integridad y Disponibilidad de la Información por malware en plataforma de servidores por falta de gestión de vulnerabilidades y buenas prácticas de aseguramiento en sistemas operativos, bases de datos y/o aplicaciones.	Realizar gestión de vulnerabilidades tecnicas sobre servidor. / / / /	13/01/2026	17/06/2026	Grupo TIC / / / /
GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	**R21**	PERDIDA DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD	SF38- Perdida de Confidencialidad, Integridad y Disponibilidad de la Información por malware en plataforma de servidores por falta de gestión de vulnerabilidades y buenas prácticas de aseguramiento en sistemas operativos, bases de datos y/o aplicaciones.	Realizar gestión de vulnerabilidades técnicas sobre servidor. / / / /	13/01/2026	17/02/2026	Grupo TIC / / / /

PROCESO	GRUPO DE TRABAJO	ID	RIESGO	CAUSA	ACCIONES ASOCIADAS AL CONTROL	Fecha Inicio	Fecha Terminación	RESPONSABLE
GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	R22	PERDIDA DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD	SF38- Perdida de Confidencialidad, Integridad y Disponibilidad de la Información por malware en plataforma de servidores por falta de gestión de vulnerabilidades y buenas prácticas de aseguramiento en sistemas operativos, bases de datos y/o aplicaciones.	Realizar gestión de vulnerabilidades técnicas sobre servidor. / / / /	13/01/2026	17/06/2026	Grupo TIC / / / /
GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	R23	PERDIDA DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD	PE03- Error en el uso. Vulnerabilidad : Capacitación insuficiente en materia de seguridad	Simular playbooks con diferentes escenarios / / / /	20/01/2026	30/12/2026	Grupo TIC / / / /

12. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la Modificación
1	29/01/2026	Versión 1 del 2025 para ser aprobado al Comité Institucional del 2025 para el 2026.
2	29/01/2026	Actualización del Plan de tratamiento de Riesgos 2025.

13. CONTROL DE FIRMAS

Elaboró	Revisó	Aprobó
Original Firmado **José Hernán Morales Muñoz** Contratista – Dirección -TIC	Original Firmado **Cristian Leonardo Cala Torres** Líder Dirección -TIC Original Firmado **Dario Alexander Méndez Beltrán** Contratista – Dirección -TIC Original Firmado **María Claudia Gonzalez** Profesional Contratista OAP	29/01/2026 **Comité Institucional de Gestión y Desempeño**