CONCEJO
DE MEDELLÍN

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

UNIDAD DE INFORMÁTICA
CONCEJO DE MEDELLÍN

2024

TABLA DE CONTENIDO

PRESENTACIÓN 3

JUSTIFICACIÓN 3

OBJETIVO 3

ALCANCE 3

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL 4

- COMPROMISO DE LA ALTA DIRECCIÓN 6
- DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN 6
- ALCANCE DE LA POLÍTICA 6
- OBJETIVO GENERAL DE LA POLÍTICA 6
- OBJETIVOS ESPECÍFICOS DE SEGURIDAD DE LA INFORMACIÓN 6
- APLICABILIDAD 7
- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y 7
- RESPONSABILIDADES) 7
- CONSECUENCIAS 8
- APROBACIÓN Y REVISIONES DE LA ALTA DIRECCIÓN 8

POLÍTICA DE GESTIÓN DEL RIESGO DEL CONCEJO DE MEDELLÍN 8

ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 9

ANÁLISIS DEL CONTEXTO ESTRATÉGICO 11

- ANÁLISIS INTERNO 12
- ANÁLISIS EXTERNO 13
- CONCLUSIÓN DEL ANÁLISIS ESTRATÉGICO 13

METODOLOGÍA DE GESTIÓN DE RIESGOS INSTITUCIONAL 14

- CRITERIOS DE EVALUACIÓN DEL RIESGO 14
- CRITERIOS PARA GESTIONAR EL RIESGO 15

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN E INFRAESTRUCTURA CRÍTICA. 15

- CLASIFICACIÓN DE ACTIVOS DE ACUERDO A LA LEY 1712 DE 2014 Y A LA LEY 1581 DE 2012 15
- CLASIFICACIÓN DE ACTIVOS DE ACUERDO A SU CRITICIDAD 19

VALORACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN 23

- IDENTIFICACIÓN DE LOS RIESGOS INHERENTES DE SEGURIDAD DE LA INFORMACIÓN 23
  - Identificación de Amenazas 23
  - Identificación de vulnerabilidades 26
  - Identificación del riesgo inherente de seguridad digital 29

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 30

CRONOGRAMA 34

SEGUIMIENTO 34

PRESENTACIÓN

El Concejo de Medellín debe definir las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma a través de la implementación del plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el conjunto de controles a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la Corporación.

Todo lo anterior se debe lograr en el marco de la normativa establecida por el Estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, emitida por el DAFP.

JUSTIFICACIÓN

La información del Concejo de Medellín como resultado del desarrollo de la misión, visión, objetivos y planes, requiere ser gestionada garantizando la presencia permanente de los atributos que acompañan su producción, organización, consulta y custodia, tales como confidencialidad, integridad y disponibilidad; los cuales deben ser analizados en los activos de información con que cuenta la Corporación, que no son más que aquellos que tienen un valor relevante dentro del sistema de gestión y los cuales se deben identificar y valorar para generar las acciones de protección necesarias que garanticen su correcto funcionamiento tanto interna como externamente.

Se debe iniciar por parte de la Corporación, la gestión de riesgos de seguridad como actividad relevante dentro de la gestión de riesgos corporativa, que permitirá proteger y cuidar los activos de información, así como identificar las debilidades y amenazas que estos tienen, generando acciones de respuesta oportuna y eficaz, que logren permitir la no materialización de los riesgos o que su impacto sea el mínimo posible.

OBJETIVO

Identificar, valorar y tratar los riesgos de seguridad y privacidad de la información, con el fin de garantizar la protección de los activos de información y la respuesta oportuna ante los eventos presentados.

ALCANCE

Incluye todos los riesgos de seguridad y privacidad que impacten a los activos de información identificados y calificados de alta criticidad en la Corporación.

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

El Concejo de Medellín, entendiendo la importancia de un adecuado manejo de la información, no solo ha definido el proceso “Gestión de la Información” dentro del mapa de procesos de la Corporación, sino que también se ha comprometido con la implementación del Modelo de Seguridad y Privacidad de la Información que promueve la estrategia de Gobierno Digital liderada por MINTIC; todo ello buscando establecer un marco de confianza en el ejercicio de sus deberes misionales, sus responsabilidades con el estado y también con los ciudadanos de Medellín; y por supuesto enmarcado en el estricto cumplimiento de las leyes en concordancia con la misión y visión de la entidad.

En el Concejo de Medellín, mediante la adopción e implementación del Modelo Integrado de Planeación y Gestión - MIPG, y específicamente del Modelo de Seguridad y Privacidad de la Información - MSPI, se protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en los procesos del Sistema de Gestión Corporativo, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales, buscando la mitigación de incidentes y el cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al mantenimiento de la privacidad y seguridad de la información. A su vez, se propende así por el acceso, uso efectivo y apropiación masiva de las TIC para el normal desarrollo del Debate Temático Público, a través de políticas y programas que favorezcan las expectativas de los grupos de valor, pero que también se mantengan alineadas con las iniciativas previstas dentro del Plan Estratégico de Tecnologías de Información – PETI.

MARCO LEGAL

Constitución Política de Colombia. Artículo 15.

Ley 44 de 1993: Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

Ley 527 de 1999: Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 594 de 2000: Por medio de la cual se expide la Ley General de Archivos.

Ley 850 de 2003: Por medio de la cual se reglamentan las veedurías ciudadanas

Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

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 de espectro y se dictan otras disposiciones.
Ley 1437 de 2011: Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
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 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos
Ley 1952 de 2019: Por medio de la cual se expide el código general disciplinario
Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto 0884 del 2012: Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886 de 2014: Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Decreto 103 de 2015: Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1074 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
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 1080 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
Decreto 1081 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia
Resolución 512 de 2019: Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información.
CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 de 2016. Política Nacional de Seguridad digital.

COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de Concejo de Medellín se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información - MSPI; así mismo, se compromete a revisar el avance de la implementación del MSPI de manera periódica y también a garantizar los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el modelo; adicionalmente, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para el Concejo de Medellín, la seguridad de la información se define como la reducción de la probabilidad o el impacto generado por un riesgo sobre los activos de información de la Corporación, identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, acorde con las necesidades de los diferentes grupos de valor de la Corporación.

ALCANCE DE LA POLÍTICA

Esta política aplica a la Corporación según como se define en el alcance del MSPI, a sus procesos, su infraestructura sus empleados, concejales, contratistas, proveedores y la ciudadanía en general,

OBJETIVO GENERAL DE LA POLÍTICA

Contribuir a la mitigación de los riesgos de seguridad de la información de todos los procesos de la Corporación, cumpliendo con los principios de confidencialidad, integridad, disponibilidad, autenticidad y no repudio; fortaleciendo la cultura de seguridad de la información y manteniendo la confianza de los grupos de valor, protegiendo los activos de información a través de políticas, procedimientos, formatos e instructivos que permitan la implementación de los controles necesarios que garanticen la continuidad de los procesos y reduzcan las probabilidades y los impactos de los incidentes; promoviendo la mejora continua y la innovación tecnológica de la Corporación, en el marco de la gestión de seguridad de la información.

OBJETIVOS ESPECÍFICOS DE SEGURIDAD DE LA INFORMACIÓN

- Minimizar los riesgos de pérdida, integridad, disponibilidad y confidencialidad de la información y garantizar la continuidad de los procesos.
- Realizar campaña de cultura en seguridad y privacidad de la información periódica para los empleados, concejales, contratistas, proveedores y ciudadanía en general que tenga relación con la Corporación.
- Realizar seguimiento al cumplimiento de la política de seguridad y privacidad de información.
- Mantener un seguimiento al manual de políticas de seguridad y privacidad de la información

- Gestionar los riesgos de seguridad y privacidad de la información, de manera integral.
- Mitigar los incidentes de Seguridad y Privacidad de la Información, de forma efectiva, eficaz y eficiente
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información de la Corporación
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

Considerándose lo anterior, el Concejo de Medellín declara que la información y sus activos asociados deben ser protegidos frente a amenazas internas o externas que puedan comprometer su confidencialidad, integridad y disponibilidad, independientemente de su formato (físico o digital).

Ante estas circunstancias, el Concejo de Medellín, ha de establecer estrategias y controles en el marco del modelo de seguridad y privacidad de la información (MSPI) que formará parte del Modelo Integrado de Planeación y Gestión (MIPG), con un enfoque basado en la gestión de riesgos y la mejora continua que busca dar cumplimiento a los requisitos legales, regulatorios, organizacionales y contractuales.

APLICABILIDAD

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a los servidores públicos y contratistas del Concejo de Medellín.

El incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la Corporación.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

La Unidad de Informática del Concejo de Medellín es el responsable designado por la Alta Dirección para desarrollar, actualizar y revisar las políticas de seguridad de la información; de acuerdo con el manual de funciones de la Corporación (Acuerdo 08 de 2015).

DESVIACIONES Y EXCEPCIONES

Desviaciones: controles de seguridad de la información definidos como inclusiones en la declaración de aplicabilidad del MSPI y que no se implementan en la Corporación.

Excepciones: se conciben como aquellos controles de seguridad de la información que son definidos como exclusiones en la declaración de aplicabilidad del MSPI y que por tanto no se implementan en la Corporación.

Todos los controles que sean incluidos en la declaración de aplicabilidad deben ser de estricto cumplimiento y aquellos que sean excluidos deben tener su justificación asociada al respectivo riesgo que pueda o no representar para la Corporación acorde con la realidad de los procesos y el alcance del MSPI.

En los casos donde se deban declarar nuevas desviaciones o excepciones, la Corporación deberá realizar una modificación a la declaración de aplicabilidad del MSPI considerando lo que ello represente en mantener la coherencia para el alcance del MSPI y la metodología de gestión de riesgo adoptada.

CONSECUENCIAS

Cualquier violación a las políticas de seguridad de la información del Concejo de Medellín debe ser sancionada de acuerdo con las normas y leyes del ordenamiento jurídico colombiano y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de la misma.

APROBACIÓN Y REVISIONES DE LA ALTA DIRECCIÓN

La Alta Dirección acepta la presente política y se compromete a destinar los recursos necesarios para la implementación, mantenimiento y mejora del Modelo de Seguridad y Privacidad del Concejo de Medellín.

Esta política será efectiva desde su aprobación por el Comité de Gestión y Desempeño. La revisión de esta política se hará en las siguientes condiciones:

- De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
- Si se dan cambios estructurales en la entidad (restructuración de áreas o procesos).
- Incidentes de seguridad de la información que requieran que la política cambie.

POLÍTICA DE GESTIÓN DEL RIESGO DEL CONCEJO DE MEDELLÍN

El Concejo de Medellín conocedor de la importancia de administrar los riesgos asociados a los objetivos estratégicos, procesos y proyectos relacionados con la operación de la Corporación, implementa su Sistema de Gestión de Riesgos como herramienta estratégica que permite anticipar y responder de manera oportuna y óptima a dichos riesgos, contribuir al cumplimiento de los objetivos y aprovechar al máximo los recursos destinados a planes, programas, y proyectos, siempre bajo las mejores condiciones de eficacia, eficiencia y efectividad.

ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La presente sección describe los roles y responsabilidades de los encargados de la Seguridad y Privacidad de la información de los diferentes procesos del Concejo de Medellín, para promover la preservación de la confidencialidad, integridad y disponibilidad de los activos de Información de la Corporación en el marco del Modelo de Seguridad y Privacidad de la Información MSPI

DEFINICIÓN DE ROLES Y RESPONSABILIDADES

La identificación de los roles y responsabilidades de seguridad de la información en el Concejo de Medellín, permite establecer al interior de la entidad las acciones correspondientes para proteger los activos de información, reduciendo posibles eventos y/o incidentes de seguridad de la información. De esta manera los colaboradores de la Corporación, adquieren el compromiso de protegerlos y se hacen partícipe de las actividades e iniciativas encaminadas al aseguramiento de los recursos que se encuentran bajo su custodia.

IDENTIFICACIÓN DE LOS RESPONSABLES

Para lograr el buen funcionamiento del Modelo de Seguridad y Privacidad de la Información MSPI, la Corporación define los roles y responsabilidades de los colaboradores de la entidad que se van a encargar de establecer y desarrollar cada una de estas actividades asociadas a los sistemas.

Para la asignación de los responsables, la Unidad de Informática del Concejo de Medellín, analiza las funciones de cada rol acorde con la **Guía de Roles y Responsabilidad V 4.0 del MinTIC** relacionándolas con las actividades que realiza el personal de la Corporación, por lo anterior, es necesario que las responsabilidades asignadas en el desarrollo del Modelo de Seguridad y Privacidad de la Información, para cada perfil o contrato, sean incorporadas a los manuales de funciones y/o en las obligaciones contractuales por prestación de servicios de acuerdo con el cargo, rol o servicio que desempeñan.

Se toma como referencia la figura del *"Equipo de Gestión de Seguridad de la Información en las entidades"* proporcionada por la **Guía de Roles y Responsabilidades V 4.0 del MinTIC**

A continuación, se definen algunos roles y responsabilidades que se toman en cuenta en la implantación y seguimiento del Modelo de Seguridad y Privacidad de la Información para el Concejo de Medellín

ROLES Y RESPONSABILIDADES

RECURSO	ROL	RESPONSABILIDAD
Comité Institucional de gestión y desempeño	Alta Dirección	Apoyo implementación MSPI Gestión Estratégica
Profesional especializado (Abogado)	Responsable asuntos jurídicos MSPI	Asesoría en temas jurídicos y legales
Subsecretaría de Despacho	Responsable asuntos talento humano MSPI	Controlar y salvaguardar datos personales
Comité de Seguridad y Privacidad de la Información	Toma de decisiones del MSPI	Toma de decisiones frente a la seguridad de la información
Responsable de seguridad de la información	Responsable MSPI	Liderazgo y responsabilidad del MSPI Gestión estratégica y táctica
Responsable del tratamiento de datos personales	Responsable MSPI	Realizar el tratamiento de datos personales acorde a la ley 1581 de 2012
Líder de la Unidad de Informática	Responsable MSPI	Apoyo técnico desde la Unidad de Informática del Concejo de Medellín a la gestión estratégica y táctica

RECURSO	ROL	RESPONSABILIDAD
		del MSPI
Grupos de Valor	Cumplimiento MSPI.	Dar estricto cumplimiento a lo estipulado en el MSPI.
Proveedores y Contratistas	Cumplimiento MSPI.	Dar estricto cumplimiento a lo estipulado en el MSPI.
Mesa de ayuda Nivel I	Apoyo operativo de las actividades requeridas del MSPI	Gestión operativa, atención y apoyo a la atención de asuntos relacionados con incidentes o con el mantenimiento de seguridad de la información.
Mesa de ayuda Nivel II	Apoyo operativo de las actividades requeridas del MSPI	Gestión operativa y apoyo al Responsable de Seguridad de la Información o quien haga sus veces.

ANÁLISIS DEL CONTEXTO ESTRATÉGICO

ANÁLISIS DOFA	
DEBILIDADES	**OPORTUNIDADES**
● Usuarios no capacitados en el uso de herramientas tecnológicas ● Falta de uso y apropiación de los sistemas de información. ● Falta de continuidad en proyectos por cambios administrativos. ● Desarticulación de la información en los procesos. ● Falta de presupuesto ● Divulgación o tratamiento inapropiada de la información ● Nivel medio de cultura organizacional frente a la seguridad y privacidad de la información. ● Inadecuada estructura organizacional ● Falta gestión del conocimiento ● Planeación institucional deficiente ● Falta de liderazgo en la gestión de la información al interior de los diferentes procesos y dependencias. ● Falta de control de acceso a los espacios destinados para los	● Apoyo por parte de la Alcaldía de Medellín en el fortalecimiento tecnológico y de seguridad. ● Soluciones tecnológicas que ofrece el mercado. ● Política de gobierno digital (MSPI) ● Fase de planificación del Modelo de Seguridad y Privacidad de la Información completada. ● Inicio de la etapa de implementación del modelo de Seguridad y Privacidad de la información ● MIPG (metodologías) ● Aplicación de cambios normativos

equipos de telecomunicaciones y redes en las instalaciones del Concejo de Medellín. ● Acceso no controlado a las instalaciones y a la información ● Factores de riesgo Psicosocial de las personas que ingresan y permanecen en el Concejo de Medellín. ● Baja gestión del riesgo de seguridad y privacidad de la información ● Baja difusión de políticas, proyectos de la gestión tecnológica. ● Ausencia de un plan de continuidad de negocio y recuperación ante desastres	
FORTALEZAS	**AMENAZAS**
● Mesa de ayuda de segundo nivel ● Equipo humano de la Unidad de informática (tecnológico) ● Sistemas de información (Orfeo, SIMI, Isolución) ● Modelo de Seguridad y Privacidad de la información documentado ● Nueva política de seguridad y privacidad de la información aprobada por la alta dirección ● Manual de políticas de seguridad de la información documentado ● Procedimientos de seguridad y privacidad de la información actualizados. ● Migración del servicio de correo electrónico a la nube de Office365 ● Migración de servidores virtuales a nuevo entorno basado en VmWare ● Infraestructura tecnológica y física. ● Gestión documental ubicada en la Unidad de informática ● Medios de difusión	● No apoyo de la alcaldía de Medellín ● Ataques cibernéticos ● Alteraciones de orden público ● Cambios normativos ● Eventos catastróficos ● Obsolescencia de equipos tecnológicos ● Vencimiento o inadecuada gestión de licenciamientos tecnológicos. ● Cambios en la TRM para adquisición de tecnología

ANÁLISIS INTERNO

Entre las FORTALEZAS se destaca la continua y oportuna gestión realizada desde la Unidad de Informática en lo referente a soporte tecnológico, gestión de la información y gestión documental. También se considera fortaleza contar con la infraestructura tecnológica y física actual que ha venido evolucionando, y con los sistemas de información que permiten la administración, procesamiento, almacenamiento y distribución de la información de los diferentes procesos de la Corporación.
Se destacan además los siguientes logros del último año:

- Modelo de Seguridad y Privacidad de la información documentado
- Nueva política de seguridad y privacidad de la información aprobada por la alta dirección

- Manual de políticas de seguridad de la información documentado
- Procedimientos de seguridad y privacidad de la información actualizados.
- Migración del servicio de correo electrónico a la nube de Office365
- Migración de servidores virtuales a nuevo entorno basado en VmWare

Las DEBILIDADES identificadas se despliegan desde lo administrativo de la Corporación hasta lo operativo de cada proceso:

- En lo administrativo se encuentran problemas de liderazgo y planeación que no permiten promover una adecuada gestión de la información y dar continuidad a proyectos de importancia en materia de seguridad y privacidad de la misma.
- En lo operativo se identifica un nivel bajo de gestión del conocimiento al interior de cada proceso que se refleja en el uso no apropiado de herramientas tecnológicas y sistemas de información, dificultando así, la gestión oportuna de los riesgos de seguridad y privacidad de la información.
- Desde la perspectiva de TI está identificada la ausencia de un plan de continuidad de negocio y recuperación ante desastres.

ANÁLISIS EXTERNO

Las AMENAZAS identificadas se relacionan con los cambios normativos, con los eventos externos que pueden afectar el funcionamiento de los sistemas y con las dificultades que se puedan presentar al momento de gestionar recursos, para financiar los proyectos en materia de seguridad y privacidad de la información.

Entre las amenazas se encuentra identificado lo siguiente

- Es importante gestionar los riesgos de seguridad informática asociados a posibilidad de ataque cibernético, dada la dinámica reciente de ataques que se ha registrado a diversidad de sectores en la economía colombiana.
- En algunos aspectos tecnológicos se identifican los riesgos de obsolescencia de equipos y el vencimiento de licenciamientos tecnológicos.

En cuanto a las OPORTUNIDADES analizadas, se considera de gran ayuda para la gestión de la seguridad y privacidad de la información, contar con los modelos, guías metodológicas y políticas definidas desde las diferentes entidades del sector público (MinTIC, DAFP), así como contar con el apoyo de un aliado estratégico como lo es la Alcaldía de Medellín.
Luego de tener un panorama más claro de lo interno y externo, se procede a desarrollar cada uno de los elementos propios de la gestión del riesgo de seguridad y privacidad de la información.

CONCLUSIÓN DEL ANÁLISIS ESTRATÉGICO
Considerando la manera en que funciona la Corporación, se analizaron factores internos y externos para diagnosticar el estado actual de la gestión en materia de seguridad de la información. Desde el análisis de lo interno se identificaron fortalezas y debilidades, y del análisis externo se identificaron oportunidades y amenazas.

METODOLOGÍA DE GESTIÓN DE RIESGOS INSTITUCIONAL

El Concejo de Medellín adopta la metodología de gestión de riesgos definida por el Departamento Administrativo de la Función Pública DAFP en la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 4 (Octubre 2018)* en el marco de las actividades para gestionar los riesgos de seguridad de la información que se enmarcan dentro del Modelo de Seguridad y Privacidad de la Información MSPI.

CRITERIOS DE EVALUACIÓN DEL RIESGO

Se adoptan los criterios de impacto y probabilidad que ofrece la Guía para la administración del riesgo del DAFP (Versión 4)

Impacto

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
MODERADO	3	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	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.
MAYOR	4	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	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.
CATASTRÓFICO	5	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	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.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. 2017

Probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

CRITERIOS PARA GESTIONAR EL RIESGO

Los riesgos de seguridad y privacidad de los activos de información, se gestionarán conforme a lo definido a la política para la gestión del riesgo de la Corporación

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN E INFRAESTRUCTURA CRÍTICA.

Los activos de información e infraestructura crítica del Concejo de Medellín se identifican
y clasifican teniendo en cuenta el valor agregado que aportan al proceso y que requieren
ser protegidos de potenciales riesgos.
Las etapas son:

- Determinar o identificar qué activos de información van a hacer parte del Inventario, que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos.
- Clasificar los activos de información de acuerdo con los tres principios de seguridad de la información, integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados.

CLASIFICACIÓN DE ACTIVOS DE ACUERDO A LA LEY 1712 DE 2014 Y A LA LEY 1581 DE 2012

TIPO DE ACTIVO	NOMBRE	PROCESO	PROPIETARIO	CUSTODIO	Ley 1712 de 2014	Ley 1581 de 2012
Información	Proyectos de acuerdo	DTP	DTP	DTP	Pública	No
	Acuerdos				Pública	N/A

TIPO DE ACTIVO	NOMBRE	PROCESO	PROPIETARIO	CUSTODIO	Ley 1712 de 2014	Ley 1581 de 2012
	Actas de sesiones plenarias				Pública	N/A
	Comisiones accidentales				Pública	N/A
	Resoluciones	DTP, GEP, GTH	DTP, GEP, GTH	DTP, GEP, GTH	Pública	Sí
	Comunicaciones oficiales	TODOS	TODOS	TODOS	Pública	Sí
	Circulares	DTP	DTP	DTP	Pública	No
	Sistema de gestión corporativo	GEP	GEP	GEP	Pública	No
	Base de datos SIMI (MySQL)	DTP	DTP	GI	Pública	No
	Base de datos Orfeo (Postgresql)	TODOS	TODOS	GI	Pública	Sí
	Base de datos Isolución (SQLServer)	TODOS	TODOS	GI	Pública	Sí
	Base de datos Regisim (Access)	GTH	GTH	GI	Pública	Sí
	Base de datos ABCD (MySQL)	CRC	CRC	GI	Pública Clasificada	Sí
	Base de datos Sivic (SQLServer)	GBS	GBS	GI	Pública	Sí
	Base de datos ZTKBioSecurity (Postgresql)	GBS	GBS	GI	Pública Clasificada	Sí
	Base de datos Sitio Web y sus micrositios (MySQL)	CRC	CRC	GI	Pública	N/A
	Archivos de configuración de dispositivos de networking	GI	GI	GI	Pública Clasificada	No

TIPO DE ACTIVO	NOMBRE	PROCESO	PROPIETARIO	CUSTODIO	Ley 1712 de 2014	Ley 1581 de 2012
Hardware	Servidores físicos	GI	GI	GI	N/A	N/A
	Firewall Perimetral Fortinet			GI	N/A	N/A
	Switches			GI	N/A	N/A
	Routers			GI	N/A	N/A
	Access point			GI	N/A	N/A
	Computadores de escritorio			GI	N/A	N/A
	Computadores portátiles			GI	N/A	N/A

TIPO DE ACTIVO	NOMBRE	PROCESO	PROPIETARIO	CUSTODIO	Ley 1712 de 2014	Ley 1581 de 2012
	Impresoras			GI	N/A	N/A
	Escáner			GI	N/A	N/A
	Cámaras fotográficas	CRC	CRC	GI	N/A	N/A
	Micrófonos	DTP	DTP	GI	N/A	N/A
	Amplificadores			GI	N/A	N/A
	Parlantes			GI	N/A	N/A
	Workstation			GI	N/A	N/A
	Matríz Netmax			GI	N/A	N/A
	Biométricos			GI	N/A	N/A
	Unidades Dicentis			GI	N/A	N/A
	Cámaras Bosch			GI	N/A	N/A
	Anycast Touch			GI	N/A	N/A
	Tv One			GI	N/A	N/A
	Encoder			GI	N/A	N/A
	Pantallas video wall			GI	N/A	N/A
	Cabinas de sonido			GI	N/A	N/A
	Teléfonos IP			GI	N/A	N/A
	Gateway Telefónico G450 Avaya			GI	N/A	N/A
	Spark Board 55"			GI	N/A	N/A
	Grabadoras de periodista			GI	N/A	N/A
	Pedales transcripción			GI	N/A	N/A

TIPO DE ACTIVO	NOMBRE	PROCESO	PROPIETARIO	CUSTODIO	Ley 1712 de 2014	Ley 1581 de 2012
Software	Windows Server	GI	GI	GI	N/A	N/A
	Windows 10			GI	N/A	N/A
	Windows 7			GI	N/A	N/A
	Servidores virtuales VMWare			GI	N/A	N/A

TIPO DE ACTIVO	NOMBRE	PROCESO	PROPIETARIO	CUSTODIO	Ley 1712 de 2014	Ley 1581 de 2012
	Servidores virtuales Proxmox			GI	N/A	N/A
	Linux RedHat			GI	N/A	N/A
	Microsoft Office 2013 (25), 2016 (94), 2019 (140), 2021(3)			GI	N/A	N/A
	Adobe creative cloud	CRC	CRC	GI	N/A	N/A
	Photoshop			GI	N/A	N/A
	Sistema de Información misional SIMI	DTP	DTP	GI	N/A	N/A
	Orfeo (Gestión Documental)	GI	GI	GI	N/A	N/A
	Isolución (Sistema de Gestión de Calidad)	GEP	GEP	GI	N/A	N/A
	Regisim (Contratos de prestación de servicios)	GTH	GTH	GI	N/A	N/A
	Metting recorder Bosch (Transcripciones)	DTP	DTP	GI	N/A	N/A
	Dicentis	DTP	DTP	GI	N/A	N/A
	IrisNet	DTP	DTP	GI	N/A	N/A
	Timesoft	GTH	GTH	GI	N/A	N/A
	ZKT Security	GTH	GTH	GI	N/A	N/A
	Sivic	GTH	GTH	GI	N/A	N/A

TIPO DE ACTIVO	NOMBRE	PROCESO	PROPIETARIO	CUSTODIO	Ley 1712 de 2014	Ley 1581 de 2012
Servicios	Sitio web y sus micrositios	CRC	CRC	GI	Pública	N/A
	Portal de Intranet	CRC	CRC	GI	Pública	N/A
	Unidades de red compartidas	GI	GI	GI	Pública	N/A
	Certificados de sitio seguro	GI	GI	GI	N/A	N/A
	Internet Dedicado Concejales (Wifi) - BW 800Mbps	DTP	DTP	GI	N/A	N/A
	Internet Banda Ancha Corporativo (Wifi) - BW 300Mbps	TODOS	TODOS	GI	N/A	N/A
	Internet Banda Ancha Visitantes (Wifi) - BW 200 Mbps	TODOS	TODOS	GI	N/A	N/A

TIPO DE ACTIVO	NOMBRE	PROCESO	PROPIETARIO	CUSTODIO	Ley 1712 de 2014	Ley 1581 de 2012
	Internet Banda Ancha Comunicaciones - BW 20Mbps	CRC	CRC	GI	N/A	N/A
	Internet Dedicado Recinto - BW 70 Mbps	DTP	DTP	GI	N/A	N/A
	Internet Móvil Concejales - 4G - Transferencia 50GB	DTP	DTP	GI	N/A	N/A
	Impresión	TODOS	GI	GI	N/A	N/A
	Internet dedicado navegación Corporativo (Cableado) - 100Mbps	TODOS	GI	GI	N/A	N/A
	Correo electrónico Microsoft Office 365	TODOS	TODOS	GI	Pública	N/A
	SAP	GEP, GTH, GBS	GEP, GTH, GBS	GI	N/A	N/A
	Herramienta colaborativa (Webex)	TODOS	TODOS	GI	N/A	N/A
Instalaciones	Centro de cableado	GI	GI	GI	N/A	N/A

CLASIFICACIÓN DE ACTIVOS DE ACUERDO A SU CRITICIDAD

TIPO DE ACTIVO	NOMBRE	Criticidad respecto a su confidencialidad	Criticidad respecto a su integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Información	Proyectos de acuerdo	Baja	Alta	Alta	Alta
	Acuerdos	Baja	Alta	Alta	Alta
	Actas de sesiones plenarias	Baja	Alta	Alta	Alta
	Comisiones accidentales	Baja	Alta	Alta	Alta
	Resoluciones	Media	Alta	Alta	Alta
	Comunicaciones oficiales	Media	Alta	Alta	Alta
	Circulares	Baja	Alta	Alta	Media
	Sistema de gestión corporativo	Baja	Alta	Alta	Media
	Base de datos SIMI (MySQL)	Baja	Alta	Alta	Media
	Base de datos Orfeo (Postgresql)	Media	Alta	Alta	Alta
	Base de datos Isolución (SQLServer)	Baja	Alta	Alta	Media

TIPO DE ACTIVO	NOMBRE	Criticidad respecto a su confidencialidad	Criticidad respecto a su integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
	Base de datos Regisim (Access)	Media	Alta	Alta	Alta
	Base de datos ABCD (MySQL)	Media	Media	Media	Media
	Base de datos Sivic (SQLServer)	Baja	Alta	Media	Media
	Base de datos ZTKBioSecurity (Postgresql)	Alta	Alta	Media	Alta
	Base de datos Sitio Web y sus micrositios (MySQL)	Baja	Alta	Alta	Alta
	Archivos de configuración de dispositivos de networking	Media	Alta	Media	Media

TIPO DE ACTIVO	NOMBRE	Criticidad respecto a su confidencialidad	Criticidad respecto a su integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Hardware	Servidores físicos	N/A	Alta	Alta	Alta
	Firewall Perimetral Fortinet	N/A	Alta	Alta	Alta
	Switches	N/A	Alta	Alta	Alta
	Routers	N/A	Alta	Alta	Alta
	Access point	N/A	Alta	Alta	Alta
	Computadores de escritorio	N/A	Alta	Media	Media
	Computadores portátiles	N/A	Alta	Media	Media
	Impresoras	N/A	Alta	Alta	Alta
	Escáner	N/A	Alta	Alta	Alta
	Cámaras fotográficas	N/A	Alta	Baja	Media
	Micrófonos	N/A	Alta	Alta	Alta
	Amplificadores	N/A	Alta	Alta	Alta
	Parlantes	N/A	Alta	Alta	Alta
	Workstation	N/A	Alta	Alta	Alta
	Matríz Netmax	N/A	Alta	Alta	Alta
	Biométricos	N/A	Alta	Media	Media

TIPO DE ACTIVO	NOMBRE	Criticidad respecto a su confidencialidad	Criticidad respecto a su integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
	Unidades Dicentis	N/A	Alta	Alta	Alta
	Cámaras Bosch	N/A	Alta	Alta	Alta
	Anycast Touch	N/A	Alta	Alta	Alta
	Tv One	N/A	Alta	Alta	Alta
	Encoder	N/A	Alta	Alta	Alta
	Pantallas video wall	N/A	Alta	Media	Alta
	Cabinas de sonido	N/A	Alta	Alta	Alta
	Teléfonos IP	N/A	Alta	Media	Media
	Gateway Telefónico G450 Avaya	N/A	Alta	Media	Media
	Spark Board 55"	N/A	Media	Media	Media
	Grabadoras de periodista	N/A	Alta	Alta	Alta
	Pedales transcripción	N/A	Alta	Alta	Alta

TIPO DE ACTIVO	NOMBRE	Criticidad respecto a su confidencialidad	Criticidad respecto a su integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Hardware	Servidores físicos	N/A	Alta	Alta	Alta
	Firewall Perimetral Fortinet	N/A	Alta	Alta	Alta
	Switches	N/A	Alta	Alta	Alta
	Routers	N/A	Alta	Alta	Alta
	Access point	N/A	Alta	Alta	Alta
	Computadores de escritorio	N/A	Alta	Media	Media
	Computadores portátiles	N/A	Alta	Media	Media
	Impresoras	N/A	Alta	Alta	Alta
	Escáner	N/A	Alta	Alta	Alta
	Cámaras fotográficas	N/A	Alta	Baja	Media
	Micrófonos	N/A	Alta	Alta	Alta
	Amplificadores	N/A	Alta	Alta	Alta
	Parlantes	N/A	Alta	Alta	Alta

TIPO DE ACTIVO	NOMBRE	Criticidad respecto a su confidencialidad	Criticidad respecto a su integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
	Workstation	N/A	Alta	Alta	Alta
	Matríz Netmax	N/A	Alta	Alta	Alta
	Biométricos	N/A	Alta	Media	Media
	Unidades Dicentis	N/A	Alta	Alta	Alta
	Cámaras Bosch	N/A	Alta	Alta	Alta
	Anycast Touch	N/A	Alta	Alta	Alta
	Tv One	N/A	Alta	Alta	Alta
	Encoder	N/A	Alta	Alta	Alta
	Pantallas video wall	N/A	Alta	Media	Alta
	Cabinas de sonido	N/A	Alta	Alta	Alta
	Teléfonos IP	N/A	Alta	Media	Media
	Gateway Telefónico G450 Avaya	N/A	Alta	Media	Media
	Spark Board 55"	N/A	Media	Media	Media
	Grabadoras de periodista	N/A	Alta	Alta	Alta
	Pedales transcripción	N/A	Alta	Alta	Alta

TIPO DE ACTIVO	NOMBRE	Criticidad respecto a su confidencialidad	Criticidad respecto a su integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Servicios	Sitio web y sus micrositios	Baja	Alta	Alta	Alta
	Portal de Intranet	Baja	Alta	Media	Media
	Unidades de red compartidas	Media	Alta	Alta	Media
	Certificados de sitio seguro	Alta	Alta	Alta	Media
	Internet Dedicado Concejales (Wifi) - BW 800Mbps	N/A	Alta	Alta	Media
	Internet Banda Ancha Corporativo (Wifi) - BW 300Mbps	N/A	Alta	Alta	Media
	Internet Banda Ancha Visitantes (Wifi) - BW 200 Mbps	N/A	Alta	Alta	Alta
	Internet Banda Ancha Comunicaciones - BW 20Mbps	N/A	Alta	Alta	Alta

TIPO DE ACTIVO	NOMBRE	Criticidad respecto a su confidencialidad	Criticidad respecto a su integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
	Internet Dedicado Recinto - BW 70 Mbps	N/A	Alta	Alta	Alta
	Internet Móvil Concejales - 4G - Transferencia 50GB	N/A	Alta	Alta	Media
	Impresión	N/A	Media	Alta	Media
	Internet dedicado navegación Corporativo (Cableado) - 100Mbps	N/A	Alta	Alta	Media
	Correo electrónico Microsoft Office 365	Media	Alta	Alta	Alta
	SAP	Alta	Alta	Alta	Alta
	Herramienta colaborativa (Webex)	Baja	Baja	Alta	Alta
Instalaciones	Centro de cableado	N/A	Alta	Alta	Alta

VALORACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

IDENTIFICACIÓN DE LOS RIESGOS INHERENTES DE SEGURIDAD DE LA INFORMACIÓN

Identificación de Amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas).

Tipo	Amenaza	Origen
Daño Físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E

Tipo	Amenaza	Origen
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las	Error en el uso	A

Tipo	Amenaza	Origen
funciones	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E
Humanas	Piratería	D
	Ingeniería social	D
	Intrusión, accesos forzados al sistema	D
	Acceso no autorizado al sistema	D
	Crimen por computador (por ejemplo, espionaje cibernético)	D
	Acto fraudulento (por ejemplo, repetición, personificación, interceptación)	D
	Soborno de la información	D
	Suplantación de identidad	D
	Intrusión en el sistema	D
	Bomba/terrorismo	D
	Guerra de la información (warfare)	D
	Ataques contra el sistema (por ejemplo, negación distribuida del servicio)	D
	Penetración en el sistema	D
	Manipulación del sistema	D
	Ventaja de defensa	D
	Ventaja Política	D
	Explotación económica	D
	Hurto de información	D
	Intrusión en la privacidad personal	D
	Ingeniería social	D
	Penetración en el sistema	D
	Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)	D
	Asalto a un empleado	D

Tipo	Amenaza	Origen
	Chantaje	D
	Observar información reservada	D
	Uso inadecuado del computador	D
	Fraude y hurto	D
	Soborno de información	D
	Ingreso de datos falsos o corruptos	D
	Interceptación	D
	Código malicioso (por ejemplo, virus, bomba lógica, troyano)	D
	Venta de información personal	D
	Errores en el sistema (bugs)	D
	Intrusión al sistema	D
	Sabotaje del sistema	D
	Acceso no autorizado al sistema	D

Identificación de vulnerabilidades

Las vulnerabilidades son defectos o debilidades de un activo. Las amenazas pueden desencadenar o explotar una vulnerabilidad para comprometer algún aspecto del activo

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencia de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de niveles del servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado

Identificación del riesgo inherente de seguridad digital

De acuerdo con lo establecido en la política para la gestión de riesgos en la Corporación, se realiza la identificación del riesgo inherente conforme a la Guía para la administración del riesgo del DAFP, versión 4.

Se identifican los siguientes riesgos inherentes de seguridad de la información:

- **Pérdida de la confidencialidad** Se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados)
- **Pérdida de la integridad** Se refiere a la exactitud y completitud de la información
- **Pérdida de la disponibilidad** Se refiere a que la información debe ser accesible y utilizable por solicitud de una persona, entidad o proceso autorizada cuando así sea requerido

Se definen categorías para agrupar los activos de información para identificar los riesgos inherentes asociados a su naturaleza, realizar el cálculo de la solidez de los controles existentes, calcular el riesgo residual luego proponer actividades de control aplicables a la categoría de activo que se registran en el plan de tratamiento. Todo esto de acuerdo a lo establecido en la guía de administración del riesgo del DAFP versión 4

Todo este flujo de actividades se registra en la matriz de riesgos de la Corporación y la calificación de la solidez de los controles.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

ID	Activos	Control	Actividad/Acción	Soporte/Evidencias	Responsable	Tiempo
1	Proyectos de acuerdo, acuerdos, resoluciones, actas de sesiones plenarias, comisiones accidentales, comunicaciones oficiales, circulares, sistema de gestión corporativo	1. Backup de información digital (SIMI, Orfeo y Isolución)	1. Cronograma establecido para backups 2. Implementar el plan de conservación documental 3. Implementar el plan de preservación digital	1. Contrato de Mesa de Ayuda 2. Evidencias de implementación de acuerdo al plan 3. Evidencias de implementación de acuerdo al plan	1. Líder Unidad Informática 2. Líder Unidad Informática 3. Líder Unidad Informática	1. Permanente 2. Continua durante el 2024 3. Continua durante el 2024

ID	Activos	Control	Actividad/Acción	Soporte/Evidencias	Responsable	Tiempo
2	Proyectos de acuerdo, acuerdos, resoluciones, actas de sesiones plenarias, comisiones accidentales, comunicaciones oficiales, circulares, sistema de gestión corporativo	Mantenimiento y gestión de actualizaciones en el software por parte de los proveedores	Hacer seguimiento al mantenimiento y gestión de actualizaciones en el software por parte de los proveedores (SIMI, Mercurio, Isolución)	Contrato con cada proveedor	Proveedor de la aplicación (SIMI, Mercurio, Isolución)	Semestral
3	Base de datos SIMI, Base de datos Mercurio, Base de datos Isolucion, Base de datos Regisim, ABCD, Sivic, ZKTBiometric, Sitio Web, Archivos networking	Mantenimiento y gestión de actualizaciones en las bases de datos por parte de los proveedores	Realizar el mantenimiento y gestión de actualizaciones en las bases de datos por parte de los proveedores (SIMI, Mercurio, Isolución, sitio web e Intranet)	Informe de mantenimiento, actualización, depuración o desfragmentación de la base de datos	Proveedor de la aplicación (SIMI, Mercurio, Isolución, sitio web e Intranet)	Semestral
4	Base de datos SIMI, Base de datos Mercurio, Base de datos Isolucion, Base de datos Regisim, ABCD, Sivic, ZKTBiometric, Sitio Web, Unidades de red	Gestión de identidades y privilegios de acceso basado en perfiles y roles	Crear perfiles y permisos basados en roles de usuario en las bases de datos de las aplicaciones.	Informe de perfiles y roles creados y depurados en el periodo.	Proveedor que administra la base de datos	Semestral
5	Servidores físicos,Firewall Perimetral, Switches, Routers, Access Point, Gateway Telefónico Avaya	Contrato de mesa de ayuda con bolsa de repuestos	Incluir bolsa de repuestos de dispositivos de networking	Contrato con proveedor de mesa de ayuda que incluya bolsa de repuestos para dispositivos de networking	Supervisor del contrato	Anual
6	Computadores de Escritorio, Computadores Portátiles, Spark Board	Contrato de soporte y mantenimiento correctivo y preventivo de equipos de cómputo de usuario final	No requiere acción dada la modernización de equipos realizada en el 2023.			
7	Matriz Netmax, Unidad Dicentis, Cámaras Bosch, AnyCast Touch, Tv One, Encoder, Workstations	Capacitación al equipo técnico que opera los dispositivos del recinto, comisiones permanentes y salones de reuniones	Verificar que se desarrollen capacitaciones al personal que opera los dispositivos del recinto	Contrato con el proveedor que realiza el mantenimiento preventivo y correctivo de los equipos del recinto	Supervisor del contrato	Anual

ID	Activos	Control	Actividad/Acción	Soporte/Evidencias	Responsable	Tiempo
8	Matriz Netmax, Unidad Dicentis, Cámaras Bosch, AnyCast Touch, Tv One, Encoder, Workstations	Uso del perfil de usuario asignado para el acceso a los dispositivos	Crear perfiles y permisos basados en roles de usuario en los accesos a los dispositivos del recinto.	Informe de perfiles y roles creados y depurados en el periodo.	Mesa de ayuda	Cada vez que sea necesario dar acceso al controlador de dominio. El informe se genera de manera semestral.
9	Biométricos, Pantallas Video Wall	Asegurar la conexión de dispositivos a fuentes de corriente con voltaje regulado	Verificar la conexión de los dispositivos a fuentes de voltaje regulado.	Informe de verificación de conexiones de dispositivos a fuentes de voltaje regulado	Líder de Programa Unidad de Servicios Generales	Anual
10	Impresoras, Escáner, Biométricos de marcación	Contrato de soporte y mantenimiento de equipos periféricos con bolsa de repuestos	No requiere acción			
11	Cámaras fotográficas, micrófonos, amplificadores, parlantes, teléfonos IP, Grabadoras de periodista, pedales transcripción, Cabinas de sonido	Reemplazo de equipos periféricos	No requiere acción			
13	Windows 10, Windows 7	Contrato de mesa de ayuda con mantenimiento preventivo y correctivo de sistema operativo de equipos de cómputo.	Ejecutar los mantenimientos correctivos y preventivos	Informe de mantenimientos correctivos y preventivos en equipos de cómputo de usuario final	Mesa de ayuda	Semestral
14	Windows Server, Linux RedHat	Contrato de mesa de ayuda nivel 2 con mantenimiento preventivo y correctivo incluyendo actualizaciones de seguridad sobre los sistemas operativos de servidor	Realizar el mantenimiento preventivo y correctivo. Así mismo realizar verificación de actualizaciones a sistema operativos	Informe de mantenimientos correctivos , preventivos y actualizaciones de seguridad de los sistemas operativos de servidor	Mesa de ayuda	Semestral
15	Servidores virtuales VMWare	Contrato de mesa de ayuda nivel 2 con mantenimiento preventivo y correctivo incluyendo actualizaciones de seguridad sobre los	Realizar el mantenimiento preventivo y correctivo. Así mismo realizar verificación de actualizaciones a sistema operativos	Informe de mantenimientos correctivos , preventivos y actualizaciones de seguridad de los sistemas operativos	Mesa de ayuda	Semestral

ID	Activos	Control	Actividad/Acción	Soporte/Evidencias	Responsable	Tiempo
		sistemas operativos de servidor		de servidor		
16	Licencias Adobe Creative Cloud, Photoshop	Adquisición de licenciamiento de uso de software de herramientas de la suite de Adobe Creative Cloud	Realizar contratación de licencias de forma oportuna	Contrato de licenciamiento	Líder de Programa Unidad de Informática	Anual
17	Licencias de Microsoft Office	Adquisición de licenciamiento de uso de software de herramientas ofimáticas de Microsoft Office	Realizar contratación de licencias de forma oportuna	Contrato de licenciamiento	Líder de Programa Unidad de Informática	Anual
18	SIMI, Mercurio, Isolución, sitio web, Intranet	Auditoría de seguridad informática tipo pentesting	Realizar la contratación de una auditoría de seguridad informática de tipo pentesting caja negra	Contrato con auditor externo	Líder de Programa Unidad de Informática	Anual
19	IrisNet, Zkt Security	Contrato de mesa de ayuda con mantenimiento preventivo y correctivo de sistema operativo de equipos de cómputo.	Ejecutar los mantenimientos correctivos y preventivos del hardware	Informe de mantenimientos correctivos y preventivos del hardware	Mesa de ayuda Proveedor de soporte y mantenimiento al recinto	Semestral
20	SIMI, Mercurio, Isolución, Regisim, IrisNet, Timesoft, Zkt Security, Sivic	Pruebas de calidad sobre el software desarrollado a la medida y verificación de funcionalidad en Software as a Service	Realizar pruebas funcionales sobre los aplicativos	Informe de pruebas funcionales sobre los aplicativos	Proveedores de las aplicaciones	Cuando se realicen nuevos desarrollos
21	Sitio web e Intranet	Configuración e implementación de Web Application Firewall para proteger el sitio web de ataques conocidos. Ejecución de pruebas de seguridad tipo pentesting para identificar vulnerabilidades o fallas de configuración actuales	Realizar la adquisición de un Web Application Firewall	Contrato de Web Application Firewall	Líder de Programa Unidad de Informática	Anual
22	Sitio web e Intranet	Contratación de personal calificado para la administración del sitio web y portales con el conocimiento para la implementación de cambios	Definir perfiles para contratar el personal calificado para la administración del sitio web y portales corporativos	Perfiles definidos	Líder de Programa Unidad de Comunicaciones	Anual
23	Servicios de Internet	Implementación de un canal con redundancia para el servicio de Internet.	No requiere acción, riesgo con baja probabilidad de ocurrencia			
24	Unidades de red	Disponibilidad de hardware para reposición de equipos de telecomunicaciones Respaldo de configuraciones de los equipos de telecomunicaciones	Contrato de mantenimiento preventivo y correctivo de dispositivos de networking con bolsa de repuestos Realizar los respaldos de configuraciones de dispositivos de	Contrato con proveedor	Supervisor del contrato	Anual

ID	Activos	Control	Actividad/Acción	Soporte/Evidencias	Responsable	Tiempo
			networking			
25	Unidades de red	Sensibilización en uso adecuado de equipos y seguridad de la información	No requiere acción			
26	Microsoft 365	Capacitación en el uso de la consola de administración del servicio de correo de Microsoft365	No requiere acción			
27	Centro de cableado	Control de acceso físico a los centros cableado con autorización de la unidad de informática	Contratar la implementación de un control de acceso físico al centro de cableado	Informe de implementación de control de acceso físico al centro del cableado	Líder de Programa Unidad de Informática	Anual

CRONOGRAMA

La Unidad de informática programa el monitoreo de los controles definidos en cada uno de los riesgos de seguridad y privacidad de la Información identificados. Es realizado semestralmente y la documentación del monitoreo se dispondrá en la plataforma de seguimiento a la política de gobierno digital.

CRONOGRAMA DE MONITOREO DE RIESGOS			
ACTIVIDAD	**DESCRIPCIÓN**	**RESPONSABLE**	**FECHA DE LOGRO**
Realizar revisión de riesgos	Realizar jornada semestral para revisar y ajustar riesgos de seguridad de la información	Líder de programa, profesionales universitarios	15 de julio de 2024
			15 de diciembre de 2024
Capacitar a los usuarios	Realizar una jornada de capacitación y socialización sobre la importancia de la prevención de los riesgos y el registro de información cuando se materialice	Líder de programa, profesionales universitarios, apoyo logístico	31 de agosto de 2024

SEGUIMIENTO

La Unidad de Informática realizará seguimiento trimestral a las acciones propuestas en el presente plan y presentará los avances ante el Comité Institucional de Gestión y Desempeño.