MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Región Metropolitana Bogotá–Cundinamarca (RMBC), en cumplimiento de la normatividad vigente y de los lineamientos de la Política de Gobierno Digital, implementa el Sistema de Gestión de Seguridad de la Información mediante políticas, procedimientos y controles orientados a proteger los activos de información y fortalecer la seguridad digital institucional.

La seguridad y privacidad de la información constituyen un habilitador estratégico para la gestión institucional, la continuidad de los servicios y la generación de confianza con los ciudadanos y las demás partes interesadas. En este contexto, el presente Manual de Políticas Complementarias **establece las directrices** para proteger la confidencialidad, integridad, disponibilidad y trazabilidad de la información, en articulación con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Seguridad y Privacidad de la Información (MSPI) y la NTC ISO/IEC 27001:2022.

2. OBJETIVO

Establecer las políticas complementarias que orientan la gestión de la seguridad y privacidad de la información, con el fin de preservar la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información, promover la gestión del riesgo y fortalecer el cumplimiento de los requisitos legales y normativos aplicables.

3. ALCANCE

El presente Manual de Políticas de Seguridad Digital, Privacidad de la Información y Protección de Datos Personales aplica a la totalidad del modelo de operación por procesos de la Región Metropolitana Bogotá–Cundinamarca, incluyendo los procesos estratégicos, misionales, de apoyo y de evaluación y control.

Sus disposiciones son aplicables a todos los servidores públicos, contratistas, proveedores, terceros y demás partes interesadas que, en el ejercicio de sus funciones, obligaciones o actividades, accedan, administren, procesen, almacenen, transmitan, compartan, custodien o eliminen información institucional, o hagan uso de los recursos tecnológicos de la Entidad.

El alcance comprende los recursos humanos, administrativos, financieros, físicos, técnicos y tecnológicos que intervienen en la gestión, tratamiento y protección de la información, incluyendo los sistemas de información, aplicaciones, plataformas, bases de datos, servicios en la nube, redes de comunicaciones, equipos de cómputo, dispositivos móviles, medios de almacenamiento, infraestructura tecnológica y documentación física o electrónica.

Las disposiciones establecidas en este manual son de obligatorio cumplimiento y se aplican durante todo el ciclo de vida de la información, independientemente de su formato, ubicación,

medio de procesamiento o mecanismo de almacenamiento, desde su creación o recepción hasta su disposición final, conservación o eliminación segura.

La implementación y fortalecimiento de los controles de seguridad y privacidad podrá desarrollarse de manera progresiva y priorizada, considerando inicialmente los procesos misionales y los activos de información con mayor impacto estratégico, criticidad o nivel de exposición a riesgos, sin que esto excluya la aplicación de las políticas y lineamientos en los demás procesos institucionales.

El presente manual será revisado y actualizado cuando se presenten cambios normativos, tecnológicos, organizacionales, operativos o relacionados con los riesgos de seguridad y privacidad de la información, así como en el marco del seguimiento y la mejora continua del Modelo de Seguridad y Privacidad de la Información —MSPI— y del Sistema de Gestión de Seguridad de la Información de la Entidad.

4. DEFINICIONES

Acceso a la información pública: Derecho fundamental que tienen todas las personas para conocer y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014).

Activo de información: Información o elemento relacionado con su tratamiento que tiene valor para la entidad, incluyendo sistemas, servicios, aplicaciones, infraestructura, personas y documentación. (ISO/IEC 27001:2022).

Amenaza: Causa potencial de un incidente que puede generar daño a un activo de información o a la entidad. (ISO/IEC 27001:2022).

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar su nivel. (ISO/IEC 27001:2022).

Autorización: Consentimiento previo, expreso e informado del titular para el tratamiento de datos personales. (Ley 1581 de 2012).

Base de datos personales: Conjunto organizado de datos personales objeto de tratamiento. (Ley 1581 de 2012).

Ciberseguridad: Capacidad de proteger y defender los activos digitales, sistemas de información e infraestructura tecnológica frente a amenazas e incidentes cibernéticos.

Confidencialidad: Propiedad de la información de no estar disponible o ser divulgada a personas, entidades o procesos no autorizados. (ISO/IEC 27001:2022).

Control: Medida destinada a modificar o gestionar el riesgo. Puede incluir políticas, procedimientos, prácticas o estructuras organizacionales. (ISO/IEC 27001:2022).

Datos personales: Cualquier información vinculada o asociada a una persona natural identificada o identificable. (Ley 1581 de 2012).

Datos personales sensibles: Datos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación. (Ley 1581 de 2012).

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando sea requerida por un usuario autorizado. (ISO/IEC 27001:2022).

Gestión de incidentes de seguridad de la información: Proceso para detectar, reportar, analizar, responder y aprender de incidentes de seguridad de la información. (ISO/IEC 27001:2022).

Integridad: Propiedad de exactitud y completitud de la información. (ISO/IEC 27001:2022).

Información pública clasificada: Información sujeta a acceso restringido por involucrar derechos particulares o privados. (Ley 1712 de 2014).

Información pública reservada: Información exceptuada del acceso público por afectar intereses públicos protegidos legalmente. (Ley 1712 de 2014).

Plan de continuidad del negocio: Plan orientado a garantizar la continuidad de las funciones críticas de la entidad ante eventos que afecten su operación. (ISO/IEC 27001:2022).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar riesgos e implementar controles de seguridad de la información. (ISO/IEC 27001:2022).

Responsable del tratamiento:
Persona natural o jurídica que decide sobre la base de datos y el tratamiento de los datos personales. (Ley 1581 de 2012).

Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad y genere impacto sobre un activo de información. (ISO/IEC 27001:2022).

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/IEC 27001:2022).

Seguridad digital: Gestión de medidas para proteger los activos digitales, servicios tecnológicos y la información en entornos digitales.

Titular: Persona natural cuyos datos personales son objeto de tratamiento. (Ley 1581 de 2012).

Tratamiento de datos personales: Cualquier operación realizada sobre datos personales, como recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012).

Trazabilidad: Capacidad de identificar y seguir las acciones realizadas sobre la información o sistemas de información. (ISO/IEC 27001:2022).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una amenaza. (ISO/IEC 27001:2022).

Encargado del tratamiento: Persona natural o jurídica que realiza el tratamiento de datos personales por cuenta del responsable del tratamiento.

Transferencia: Envío de datos personales a un tercero que los recibe y actúa como nuevo responsable de su tratamiento.

Transmisión: Comunicación de datos personales a un encargado para que los trate siguiendo las instrucciones y por cuenta del responsable.

Anonimización: Proceso irreversible mediante el cual los datos se transforman de manera que el titular no pueda ser identificado, directa ni indirectamente. Los datos correctamente anonimizados dejan de considerarse datos personales.

Seudonimización: Proceso mediante el cual los datos identificativos se sustituyen por códigos, seudónimos u otros identificadores. La persona puede ser identificada nuevamente utilizando información adicional, la cual debe conservarse separada y protegida; por tanto, continúan siendo datos personales.

Activo crítico: Activo de información cuya pérdida, alteración, divulgación o indisponibilidad podría afectar gravemente la operación, los objetivos o los servicios de la entidad.

5. SIGLAS

CIGD: Comité Institucional de Gestión y Desempeño.
MinTIC: Ministerio de Tecnologías de la Información y las Comunicaciones
MSPI: Modelo de Seguridad y Privacidad de la Información
MIPG: Modelo Integrado de Planeación y Gestión
OTIC: Oficina de Tecnologías de la Información y las Comunicaciones
PETI: Plan Estratégico de Tecnologías de la Información
RMBC: Región Metropolitana Bogotá – Cundinamarca
SGSI: Sistema de Gestión de Seguridad de la Información
TIC: Tecnologías de la Información y las Comunicaciones

6. MARCO NORMATIVO

• **Resolución 0500 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 02277 de 2025,** "Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia".

• **Directiva Presidencial 02 Del 24 De febrero De 2022,** "Para garantizar la implementación segura de la política de gobierno digital liderada por La Entidad de Tecnologías de la Información y las Comunicaciones (MinTIC)".

• **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 527 de 1999, –** Por medio de 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**.**

• **CONPES 3854 de 2016,** Política Nacional de Seguridad Digital busca fortalecer, identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

• **CONPES 3995 de 2020, –** Política Nacional De Confianza y Seguridad Digital "Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías".

• **Norma técnica colombiana 27001 de 2022**, Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

• **El Modelo de Seguridad y Privacidad de la Información - MSPI**, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas.

• **Ley 1581 de 2012,** Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.

• **Decreto 338 de 2022**, establece los lineamientos generales para la gobernanza de seguridad digital, con el cual busca aunar y dinamizar el desarrollo legal, los avances técnicos, así como los conocimientos estatales y privados para fortalecer la ciberseguridad del país.

• **Resolución 1519 del 2020,** "por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".

• **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"; regula el acceso a la información pública, los procedimientos para garantizar este derecho y las excepciones a la publicidad de la información.

• **Decreto 1078 de 2015,** "por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"; compila la reglamentación del

sector TIC e incluye disposiciones relacionadas con la implementación de la Política de Gobierno Digital.

7. POLITICA GENERAL DE SEGURIDAD DIGITAL, SEGURIDAD DE LA INFORMACIÓN, PRIVACIDAD DE LA INFORMACIÓN Y PROTECCION DE DATOS PERSONALES

La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) liderará la implementación, seguimiento y actualización de estas políticas, en coordinación con las dependencias responsables y de acuerdo con el análisis de riesgos, los requisitos legales, las necesidades institucionales y el proceso de mejora continua.

Las políticas serán desarrolladas mediante procedimientos, guías, estándares técnicos y demás instrumentos que resulten necesarios para su adecuada implementación.

8. POLÍTICAS COMPLEMENTARIAS

Las políticas contenidas en el presente manual se organizan por dominios de seguridad de la información, de conformidad con el Sistema de Gestión de Seguridad de la Información (SGSI), el Modelo de Seguridad y Privacidad de la Información (MSPI), la gestión de riesgos y las necesidades de protección de los activos de información de la Entidad.

8.1. Organización Interna

Objetivo: Establecer la estructura organizacional y los lineamientos que permitan implementar, operar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) en la Región Metropolitana Bogotá–Cundinamarca.

Política:

- La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) liderará la implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), articulando su gestión con las dependencias responsables para garantizar la aplicación de las políticas, procedimientos y controles de seguridad de la información en todos los procesos de la Entidad.

8.1.1. Liderazgo de la Alta Dirección

Objetivo: Establecer el compromiso de la Alta Dirección con la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando la disponibilidad de recursos, la definición de responsabilidades y el cumplimiento de los objetivos institucionales en materia de seguridad digital.

Políticas

- Aprobar la Política General de Seguridad Digital, Seguridad de la Información, Privacidad de la Información y Protección de Datos Personales.
- Promover la implementación, mantenimiento y mejora continua del SGSI.
- Garantizar la disponibilidad de los recursos humanos, tecnológicos, financieros y organizacionales necesarios para la gestión de la seguridad de la información.
- Apoyar la gestión de los riesgos de seguridad de la información.
- Realizar, a través del Comité Institucional de Gestión y Desempeño (CIGD), la revisión periódica del desempeño del SGSI, considerando el cumplimiento de los objetivos, los indicadores, los resultados de auditoría, los incidentes de seguridad, el estado de las acciones de mejora y demás elementos necesarios para asegurar su eficacia.
- Promover la implementación y seguimiento de las acciones de mejora derivadas de las revisiones del SGSI, auditorías, incidentes de seguridad y demás mecanismos de evaluación institucional.
- Fomentar una cultura organizacional orientada a la protección de la información y al mejoramiento continuo.

Responsables

- Alta Dirección.
- Comité Institucional de Gestión y Desempeño (CIGD).

8.1.2. Roles y responsabilidades

Objetivo: Definir y asignar las responsabilidades para la gestión de la seguridad y privacidad de la información, garantizando que todos los actores involucrados conozcan y cumplan las obligaciones que les corresponden en el Sistema de Gestión de Seguridad de la Información (SGSI).

Políticas

- La gestión de la seguridad y privacidad de la información es responsabilidad de todos los servidores públicos, contratistas, proveedores, terceros y demás usuarios autorizados que administren, procesen o tengan acceso a la información y a los recursos tecnológicos de la Región Metropolitana Bogotá–Cundinamarca.

- Cada dependencia será responsable de implementar los controles de seguridad de la información que correspondan a sus procesos, proteger los activos de información bajo su custodia y cumplir las políticas, procedimientos y demás lineamientos definidos por la Entidad.

Responsables

Oficina de Tecnologías de la Información y las Comunicaciones (OTIC)

- Liderar la implementación, operación y mejora continua del SGSI.

- Definir y mantener los lineamientos, procedimientos y controles técnicos de seguridad de la información.

- Coordinar la gestión de riesgos, incidentes, vulnerabilidades y continuidad de los servicios tecnológicos.
- Promover actividades de capacitación y sensibilización en seguridad de la información.
- Responsable de la política y del manual de Seguridad de la Información
- Coordinar la implementación y seguimiento del SGSI.
- Monitorear la eficacia de los controles.
- Coordinar la gestión de riesgos e incidentes.
- Promover acciones de mejora continua.

Líderes de proceso

- Implementar los controles de seguridad definidos para los procesos bajo su responsabilidad.
- Identificar y gestionar los riesgos de seguridad de la información asociados a sus procesos.
- Velar por el cumplimiento de las políticas de seguridad por parte de su equipo de trabajo.

Dependencias de apoyo

- Las dependencias que administren información institucional deberán implementar y mantener los controles de seguridad que correspondan a sus funciones, garantizando la protección de los activos de información bajo su responsabilidad y el cumplimiento de los lineamientos definidos por la Entidad.

Servidores públicos, contratistas, proveedores, terceros y usuarios autorizados

- Cumplir las políticas y controles de seguridad de la información.
- Proteger la información y los recursos tecnológicos bajo su responsabilidad.
- Reportar oportunamente incidentes o eventos de seguridad.
- Utilizar los recursos tecnológicos de forma segura y conforme a los lineamientos institucionales.

La matriz RACI utiliza las siguientes convenciones: R = ejecuta o desarrolla; A = aprueba o responde por el resultado; C = participa o es consultado; I = recibe información. La asignación deberá ajustarse cuando un procedimiento institucional defina competencias específicas.

ACTIVIDAD	DIRECCIÓN / CIGD	OTIC	PLANEACIÓN	LÍDERES DE PROCESO	GESTIÓN CORPORATIVA	JURÍDICA	COMUNICACIONES	CONTROL INTERNO
Aprobar alcance y prioridades del MSPI	A	R	C	C	I	C	I	I

Realizar y consolidar autodiagnóstico	I	R	C	C	I	I	I	C
Identificar partes interesadas y requisitos	I	R	C	C	C	C	I	I
Identificar y clasificar activos	I	C	C	R/A	C	I	I	I
Definir metodología y matriz de riesgos	I	R	C	C	I	C	I	I
Valorar riesgos por proceso	I	C	C	R/A	I	I	I	I
Aprobar tratamiento de riesgos críticos	A	R	C	C	I	C	I	I
Elaborar Declaración de Aplicabilidad	I	R/A	C	C	I	C	I	I
Implementar controles tecnológicos	I	R/A	I	C	I	I	I	I
Implementar controles administrativos y de proceso	I	C	C	R/A	C	C	I	I
Incorporar requisitos en contratos	I	C	I	C	C	R/A	I	I
Ejecutar sensibilización y comunicación	I	R	C	C	C	C	C/A	I
Gestionar eventos e incidentes	I	R/A	I	R	C	C	I	I
Gestionar vulnerabilidades	I	R/A	I	C	I	I	I	I
Medir indicadores y consolidar informes	I	R	C	C	I	I	I	I
Realizar evaluación independiente	I	I	I	I	I	I	I	R
Aprobar y hacer seguimiento a acciones de mejora	A	R	C	R	C	C	I	C

8.1.3. Comunicación del sistema de gestión de seguridad de la información

Objetivo: Establecer los lineamientos para la comunicación interna y externa del Sistema de Gestión de Seguridad de la Información (SGSI), garantizando la divulgación oportuna de las políticas, lineamientos y responsabilidades en materia de seguridad de la información

Políticas

- Región Metropolitana Bogotá–Cundinamarca establecerá los mecanismos de comunicación interna y externa necesarios para divulgar las políticas, lineamientos y demás documentos del SGSI.
- La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) coordinará la divulgación de la información relacionada con el SGSI mediante los canales institucionales autorizados.
- Las actividades de comunicación y sensibilización se desarrollarán conforme al **PN-TIC-004** Plan de Sensibilización y Comunicación en Seguridad de la Información.
- La comunicación con servidores públicos, contratistas, proveedores y demás partes interesadas se realizará utilizando los canales oficiales definidos por la Entidad.

8.1.4. Segregación de funciones

Control 5.3 Establecer lineamientos para la segregación de funciones y responsabilidades críticas, con el fin de reducir el riesgo de fraude, errores, conflictos de interés y accesos no autorizados.

Políticas

- La Entidad implementará mecanismos de segregación de funciones cuando la naturaleza de los procesos, los riesgos identificados o la criticidad de los activos de información así lo requieran, procurando que las actividades de autorización, ejecución, revisión y control sean desempeñadas por personas o roles diferentes.
- Cuando no sea posible aplicar una segregación efectiva por limitaciones organizacionales o de recursos, la Entidad establecerá controles compensatorios que permitan reducir el riesgo asociado.

8.1.5. Contacto con autoridades

Control 5.5: Establecer los lineamientos para mantener relaciones institucionales con las autoridades competentes en materia de seguridad digital, ciberseguridad y protección de la información.

Política

- La Entidad mantendrá canales de comunicación con las autoridades y organismos competentes para facilitar la atención de incidentes, el intercambio de información y el cumplimiento de las obligaciones legales y regulatorias relacionadas con la seguridad de la información.

8.1.6. Contacto con grupo de interés especial

Control 5.6: Fortalecer la gestión de la seguridad de la información mediante la participación en redes, comunidades y organismos especializados.

Políticas

- OTIC promoverá la participación institucional en grupos de interés, comunidades técnicas, organismos especializados y foros relacionados con seguridad de la

información y ciberseguridad, con el propósito de fortalecer el conocimiento institucional, intercambiar buenas prácticas y conocer oportunamente amenazas, vulnerabilidades y recomendaciones emitidas por organismos nacionales e internacionales.

- Centro Cibernético Policial – CCP
- CAI Virtual
- Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT),
- CSIRT Presidencia y el Comando Conjunto Cibernético de las FFMM - CCOC.

8.1.7. Inteligencia de amenazas

Control 5.7: Establecer los lineamientos para identificar, analizar y utilizar información sobre amenazas de seguridad de la información y ciberseguridad que permita fortalecer la gestión preventiva del riesgo y la protección de los activos de información.

Políticas

- OTIC realizará el seguimiento permanente a fuentes de información confiables sobre amenazas, vulnerabilidades y riesgos emergentes que puedan afectar la operación de la Entidad.
- La información obtenida será analizada para determinar su aplicabilidad y, cuando corresponda, apoyar la implementación de controles, la actualización del análisis de riesgos, la gestión de incidentes y la adopción de acciones preventivas o correctivas.
- Las actividades relacionadas con la inteligencia de amenazas deberán conservar la trazabilidad necesaria que permita evidenciar su análisis y las acciones implementadas.

8.1.8. Seguridad de la información en la gestión de proyectos

Control 5.8: Incorporar la seguridad y privacidad de la información como un componente transversal durante el ciclo de vida de los proyectos institucionales.

Políticas

- Todos los proyectos institucionales deberán incorporar requisitos de seguridad y privacidad de la información acordes con su alcance, naturaleza, nivel de riesgo y tratamiento de la información.
- Cuando el proyecto contemple el desarrollo, adquisición, integración o modificación de sistemas de información o servicios tecnológicos, deberán aplicarse prácticas de desarrollo seguro, protección de datos personales, gestión de vulnerabilidades y demás controles definidos por la Entidad.

8.2. Dispositivos Móviles y Teletrabajo

Objetivo: Establecer los lineamientos para el uso seguro de dispositivos móviles y la modalidad de teletrabajo, con el fin de proteger la información institucional, reducir los riesgos asociados

al acceso remoto y garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad.

8.2.1. Política para dispositivos móviles

Control 8.1: La Entidad debe adoptar una política para uso de dispositivos móviles y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de estos dispositivos.

Políticas

- El acceso a los recursos tecnológicos institucionales desde dispositivos móviles deberá realizarse mediante conexiones seguras y mecanismos de autenticación autorizados. Se deberá utilizar autenticación multifactor cuando el servicio lo permita.
- Los dispositivos que almacenen o procesen información institucional deberán contar con mecanismos de cifrado para protegerla contra accesos no autorizados.
- Los dispositivos deberán tener habilitado el bloqueo automático por inactividad y utilizar contraseña, PIN seguro o mecanismo biométrico para su desbloqueo.
- Los usuarios serán responsables de la protección física y lógica de los dispositivos y deberán reportar inmediatamente a la OTIC cualquier pérdida, hurto, compromiso de seguridad o uso no autorizado.
- Ante el reporte de un incidente, la OTIC podrá bloquear el acceso, revocar sesiones y aplicar las medidas de contención necesarias para proteger la información institucional.
- La instalación de software, modificación de configuraciones de seguridad o utilización de herramientas no autorizadas requerirá autorización de la OTIC. No se permitirá el acceso desde dispositivos con modificaciones que eliminen las restricciones de seguridad del fabricante.

8.2.2. Teletrabajo

Control 6.7: Establecer los lineamientos de seguridad para el desarrollo de actividades bajo modalidades de teletrabajo o trabajo remoto, garantizando la protección de la información institucional y el acceso seguro a los recursos tecnológicos de la Entidad.

Políticas

- La Entidad implementará los controles de seguridad necesarios para proteger la información institucional cuando las actividades se desarrollen bajo modalidades de teletrabajo o trabajo remoto.
- Los servidores públicos, contratistas y demás personas autorizadas deberán utilizar exclusivamente los servicios tecnológicos, plataformas de colaboración y mecanismos de acceso aprobados por la Entidad para el desarrollo de sus funciones.
- Los usuarios serán responsables de proteger la información institucional a la que accedan durante el trabajo remoto y de cumplir las políticas de seguridad de la información, confidencialidad y protección de datos establecidas por la Entidad.
- La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) definirá e implementará los controles técnicos necesarios para proteger el acceso remoto a los servicios tecnológicos institucionales, de acuerdo con el análisis de riesgos y las capacidades tecnológicas disponibles.

9. SEGURIDAD DE LOS RECURSOS HUMANOS

Región Metropolitana Bogotá–Cundinamarca (RMBC) establece los lineamientos para la gestión de la seguridad y privacidad de la información durante todo el ciclo de vinculación de los servidores públicos, contratistas, proveedores y demás terceros autorizados, con el fin de promover el conocimiento de sus responsabilidades, proteger los activos de información y reducir los riesgos asociados al acceso, uso y tratamiento de la información institucional.

9.1. Antes de Asumir el Empleo

Objetivo: Garantizar que los servidores públicos, contratistas y demás terceros comprendan sus responsabilidades en materia de seguridad de la información antes de acceder a los activos de información y recursos tecnológicos de la Entidad.

9.1.1. Selección

Control 6.1: Garantizar que los servidores públicos, contratistas y demás terceros que accedan a la información institucional cumplan los requisitos de idoneidad, confiabilidad y responsabilidad, de acuerdo con las funciones que desempeñarán y los riesgos asociados.

Políticas

- La Entidad realizará las verificaciones de idoneidad, antecedentes y demás requisitos aplicables a los servidores públicos, contratistas y terceros, de acuerdo con la normatividad vigente, el nivel de responsabilidad del cargo y los riesgos asociados al acceso a la información institucional.
- Cuando la naturaleza de las funciones lo requiera, los usuarios deberán suscribir los compromisos de confidencialidad y cumplir las políticas de seguridad de la información antes de acceder a los activos de información y recursos tecnológicos de la Entidad.
- Las dependencias responsables de la vinculación deberán informar oportunamente a la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) las novedades que impliquen la creación o habilitación de accesos a los servicios tecnológicos institucionales.

9.1.2. Términos y condiciones del empleo

Control 6.2: Establecer las responsabilidades en materia de seguridad y privacidad de la información que deberán cumplir los servidores públicos, contratistas y demás terceros durante su relación laboral o contractual con la Entidad.

Política

- Los actos administrativos, contratos, convenios o demás instrumentos de vinculación deberán establecer las responsabilidades relacionadas con la seguridad y privacidad de la información, el uso adecuado de los recursos tecnológicos, la protección de los datos personales y el cumplimiento de las políticas institucionales aplicables.
- Los servidores públicos, contratistas y terceros deberán guardar reserva y confidencialidad sobre la información clasificada, reservada, los datos personales y

demás información institucional conocida con ocasión de sus funciones u obligaciones. Esta información no podrá ser divulgada, utilizada, copiada o compartida para fines distintos de los autorizados.

- El deber de reserva y confidencialidad continuará vigente después de la terminación de la relación laboral o contractual, cuando resulte aplicable conforme a la normativa y a los compromisos suscritos.

9.2. Durante la Ejecución del Empleo

Objetivo: Promover el cumplimiento permanente de las responsabilidades de seguridad de la información durante la relación laboral o contractual y fortalecer la cultura institucional de seguridad.

9.2.1. Toma de conciencia, educación y formación

Control 6.3: Fortalecer la cultura institucional de seguridad y privacidad de la información mediante actividades permanentes de sensibilización, educación y formación dirigidas a los servidores públicos, contratistas y demás terceros autorizados.

Políticas

- La Entidad promoverá la toma de conciencia, la educación y la formación en seguridad y privacidad de la información, fortaleciendo las competencias de los servidores públicos, contratistas y demás terceros para el cumplimiento de las políticas institucionales y la adecuada protección de los activos de información.

- La OTIC coordinará la ejecución y actualización del Plan de Sensibilización y Comunicación en Seguridad de la Información, conservando las evidencias de las actividades desarrolladas.

9.2.2. Procesos disciplinarios

Control 6.4: Establecer las acciones disciplinarias aplicables frente al incumplimiento de las políticas y controles de seguridad de la información, de conformidad con la normatividad vigente y los procedimientos institucionales.

Política

- La Entidad, a través de la dependencia competente, adelantará las actuaciones disciplinarias a que haya lugar cuando los servidores públicos incumplan las políticas de seguridad de la información, de conformidad con la normatividad vigente.

9.3. Terminación o Cambio de Empleo

Control 6.5: Garantizar la protección de la información y de los activos institucionales durante los procesos de cambio de funciones, suspensión, terminación o finalización de la relación laboral o contractual.

Políticas

- Durante los procesos de cambio o terminación de la relación laboral o contractual, la Entidad deberá garantizar la devolución de los activos asignados, la revocación o modificación de los accesos a los recursos tecnológicos y la transferencia de la información o de las actividades bajo responsabilidad del servidor público o contratista.

- Las obligaciones relacionadas con la confidencialidad, la protección de la información y el tratamiento de los datos personales continuarán vigentes después de la finalización de la relación laboral o contractual, cuando así lo establezcan la normatividad o los instrumentos suscritos con la Entidad.
- Las dependencias responsables, Gestión Corporativa o los supervisores de contratos deberán informar oportunamente a la OTIC las novedades administrativas que puedan afectar los accesos otorgados, incluyendo vacaciones, licencias, suspensiones, cambios de funciones, traslados y terminaciones de la vinculación.
- Recibida la notificación, la OTIC y el responsable del recurso tecnológico deberán revisar los permisos asignados y, cuando corresponda, modificarlos, suspenderlos o revocarlos, de acuerdo con las funciones vigentes, el principio de mínimo privilegio y los riesgos identificados.
- La reactivación de accesos suspendidos deberá realizarse previa validación de la finalización de la novedad y autorización de la dependencia responsable.

10. GESTIÓN DE ACTIVOS

Establece lineamientos para la gestión de los activos de información y demás activos asociados, orientados a garantizar su identificación, protección, uso adecuado y administración durante todo su ciclo de vida, mediante la asignación de responsabilidades y la aplicación de controles de seguridad de la información.

10.1. Inventario de Activos

Control 5.9: Identificar, registrar, administrar y mantener actualizado el inventario de los activos de información y demás activos asociados, garantizando la asignación de responsabilidades y la aplicación de los controles de seguridad durante todo su ciclo de vida.

Políticas

- La Entidad mantendrá un inventario actualizado de los activos de información y demás activos asociados, identificando como mínimo su propietario, clasificación, criticidad, ubicación y demás atributos necesarios para su adecuada gestión.
- La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) coordinará la administración y actualización del inventario institucional de activos de información, en articulación con los líderes de proceso y propietarios de los activos.
- Los propietarios de los activos serán responsables de mantener actualizada la información bajo su custodia y de aplicar los controles de protección definidos por la Entidad.

10.2. Propiedad de los Activos

Control 5.9 /5.12: Asignar un propietario a cada activo de información, responsable de su administración, clasificación, protección, uso y revisión durante todo su ciclo de vida, garantizando la aplicación de los controles de seguridad definidos por la Entidad.

Políticas

- Todo activo de información deberá tener un propietario formalmente designado, responsable de su clasificación, protección, actualización, definición de los requisitos de seguridad y autorización de acceso, cuando corresponda.
- Cuando se presenten cambios organizacionales o funcionales, la asignación del propietario deberá actualizarse oportunamente.

10.3. Uso Aceptable de los Activos

Control 5.10: Establecer los lineamientos para el uso adecuado de la información y de los activos asociados, garantizando su protección y utilización conforme a las funciones y las políticas de seguridad de la información.

Políticas

- Los usuarios deberán utilizar la información y los activos asociados exclusivamente para el desarrollo de las funciones y actividades institucionales autorizadas por la Entidad.
- Los usuarios serán responsables de proteger los activos asignados y de prevenir su pérdida, alteración, divulgación, uso indebido o acceso no autorizado.
- Los activos tecnológicos únicamente podrán ser administrados, configurados o intervenidos por personal autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) o conforme a los procedimientos institucionales establecidos.
- El incumplimiento de los lineamientos de uso aceptable podrá dar lugar a las acciones administrativas, disciplinarias, contractuales o legales a que haya lugar.

10.3.1. Uso de la información

Políticas

- La información institucional deberá utilizarse únicamente para el cumplimiento de las funciones y actividades autorizadas por la Entidad.
- La información que contenga datos personales deberá tratarse de conformidad con la normatividad vigente sobre protección de datos personales y las políticas institucionales.
- Toda modificación, actualización o eliminación de la información deberá realizarse por personal autorizado y, cuando corresponda, con aprobación del propietario de la información.
- Se prohíbe la reproducción, divulgación, transferencia o uso no autorizado de la información institucional.

10.3.2. Uso de equipos de cómputo

Políticas

- Los equipos de cómputo y demás recursos tecnológicos asignados por la Entidad deberán utilizarse exclusivamente para el desarrollo de las funciones y actividades institucionales autorizadas.
- Los usuarios serán responsables de la custodia, cuidado y uso adecuado de los equipos asignados, adoptando las medidas necesarias para prevenir su pérdida, daño, hurto o uso no autorizado.
- No se permitirá instalar software no autorizado, modificar las configuraciones de seguridad, deshabilitar los controles implementados por la Entidad ni realizar intervenciones técnicas sobre los equipos sin autorización previa de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC).
- Los equipos de cómputo deberán conservar los elementos de identificación e inventario asignados por la Entidad y no podrán ser retirados, trasladados o reasignados sin la autorización correspondiente.
- Los usuarios deberán reportar oportunamente a la Mesa de Servicio cualquier daño, pérdida, hurto, mal funcionamiento o incidente de seguridad que afecte los equipos bajo su responsabilidad.

10.3.3. Uso del correo electrónico y herramientas colaborativas

Políticas

- Las cuentas institucionales son personales e intransferibles. Cada usuario será responsable del uso adecuado de los servicios asignados y de las actividades realizadas mediante estos.
- La información institucional transmitida, compartida o almacenada mediante el correo electrónico o las herramientas colaborativas deberá protegerse de acuerdo con su clasificación y con los lineamientos de seguridad definidos por la Entidad.
- Los usuarios deberán utilizar únicamente las herramientas colaborativas autorizadas por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), evitando el uso de plataformas no aprobadas para el tratamiento de información institucional.
- La OTIC establecerá los lineamientos técnicos y controles necesarios para garantizar el uso seguro del correo electrónico institucional y de las herramientas colaborativas.
- Los correos electrónicos institucionales incorporarán el aviso de confidencialidad definido por la Entidad, de conformidad con los lineamientos establecidos por la OTIC.

10.3.4. Uso de internet

Políticas

- Los usuarios deberán utilizar el servicio de Internet de forma responsable y exclusivamente para el desarrollo de las funciones y actividades institucionales.
- El acceso a los servicios de Internet y a los recursos web será otorgado de acuerdo con el rol, las funciones y las necesidades del servicio de cada usuario.

- Los usuarios deberán cumplir las restricciones y controles de navegación definidos por la Entidad.
- El acceso a Internet podrá ser monitoreado por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) con fines de seguridad, continuidad del servicio, cumplimiento de las políticas institucionales y atención de incidentes de seguridad de la información.
- Se prohíbe divulgar, transmitir o almacenar información institucional, datos personales o información clasificada mediante servicios de Internet no autorizados por la Entidad.
- Cualquier evento, incidente o situación que pueda comprometer la seguridad de la información durante el uso de Internet deberá ser reportado oportunamente a la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC)

10.4. Devolución

Control 5.11: Garantizar la devolución, reasignación o disposición de los activos de información y recursos tecnológicos al finalizar o modificarse la relación laboral o contractual, asegurando la protección de la información institucional durante todo el ciclo de vida del activo.

Políticas

- Toda persona que finalice o modifique su vínculo con la Entidad deberá devolver los activos de información y recursos tecnológicos que le hayan sido asignados, conforme a los procedimientos institucionales.
- La devolución de los activos deberá garantizar la actualización de los inventarios, la revocación de los accesos y el cierre de las responsabilidades asociadas.
- Antes de la reasignación, devolución o disposición final de los activos tecnológicos, la OTIC deberá aplicar, cuando corresponda, los procedimientos de respaldo y borrado seguro de la información institucional.

10.5. Clasificación de la Información

Control 5.12: Garantizar que la información institucional sea clasificada de acuerdo con su sensibilidad, criticidad y requisitos legales, con el fin de aplicar los controles de seguridad apropiados durante todo su ciclo de vida.

Políticas

- Todo activo de información deberá ser clasificado por su propietario de acuerdo con los criterios establecidos por la Entidad y mantenerse actualizado en el inventario institucional de activos de información.
  La clasificación institucional será la siguiente:
  - Información Pública.
  - Información Pública Clasificada.
  - Información Pública Reservada.
  - Información Confidencial Institucional.
- Los líderes de proceso o propietarios de los activos deberán asegurar que la información, tanto física como digital, se encuentre **clasificada y etiquetada** de

acuerdo con su nivel de clasificación, con el fin de garantizar la aplicación de los controles de protección correspondientes.

10.6. Etiquetado

Control 5.13: Etiquetado de la información: Establecer los lineamientos para identificar la información de acuerdo con su clasificación, facilitando la aplicación de los controles de seguridad correspondientes.

Políticas

- La información clasificada deberá identificarse mediante mecanismos de etiquetado físico o digital que permitan reconocer su nivel de clasificación y aplicar los controles de protección definidos por la Entidad.
- El etiquetado deberá aplicarse de acuerdo con los lineamientos institucionales y mantenerse durante todo el ciclo de vida de la información.

10.6.1. Enmascaramiento de datos personales e información sensible

Control 8.11: Enmascaramiento de datos: Establecer los lineamientos para proteger los datos personales y la información sensible mediante técnicas de enmascaramiento, seudonimización o anonimización, cuando la naturaleza de la información, el análisis de riesgos, los requisitos legales o las necesidades operativas de la Región Metropolitana Bogotá–Cundinamarca así lo requieran.

Políticas

- OTIC, en coordinación con los propietarios de la información y los líderes de proceso, evaluará la necesidad de implementar técnicas de enmascaramiento, seudonimización o anonimización para la protección de datos personales e información sensible, de acuerdo con la clasificación de la información y el análisis de riesgos institucional.
- El tratamiento de datos personales deberá cumplir la Ley 1581 de 2012, los lineamientos institucionales de protección de datos personales y las demás disposiciones legales aplicables.
- Cuando los sistemas de información requieran ambientes de desarrollo, pruebas, capacitación, interoperabilidad o análisis estadístico, se priorizará el uso de información anonimizada, seudonimizada o enmascarada, evitando el tratamiento de datos personales reales cuando no sea estrictamente necesario.

- La implementación de mecanismos de enmascaramiento de datos deberá evaluarse previamente mediante análisis de riesgos, viabilidad técnica y requerimientos funcionales de los sistemas de información.
- Los mecanismos de enmascaramiento, seudonimización o anonimización que se implementen deberán conservar la integridad y utilidad de la información para el propósito autorizado, evitando la posibilidad de reidentificación no autorizada.
- Toda implementación de técnicas de protección de datos deberá documentarse y mantenerse bajo control de cambios conforme al **P-TIC-001** Gestionar la arquitectura de tecnología **– proceso habilitación del cambio**

10.7. Gestión de Medios

Objetivo: Establecer los lineamientos para la gestión segura de los medios de almacenamiento que contengan información institucional durante su creación, uso, almacenamiento, transporte, reutilización y disposición final, con el fin de prevenir la divulgación, modificación, pérdida, acceso no autorizado o destrucción de la información.

10.7.1. Gestión de medios removibles (Control 7.10)

Políticas

- La utilización de medios removibles deberá responder a una necesidad institucional y cumplir los controles de seguridad establecidos por la Entidad.
- Los medios removibles de propiedad de la Entidad deberán mantenerse identificados, inventariados y bajo la custodia de un responsable.
- Los usuarios serán responsables de la protección física y lógica de los medios removibles asignados y deberán prevenir su pérdida, robo, acceso no autorizado o uso indebido.
- Los medios removibles deberán protegerse de acuerdo con la clasificación de la información que contengan y con los lineamientos definidos por la Entidad.

10.7.2. Disposición segura de medios (Control 7.14)

Políticas

- Antes de la reutilización, devolución, baja o disposición final de los medios de almacenamiento o equipos tecnológicos, deberá garantizarse la eliminación segura de la información conforme a los procedimientos institucionales.
- La disposición final de los medios y equipos tecnológicos deberá realizarse de conformidad con los lineamientos institucionales para la gestión de residuos de aparatos eléctricos y electrónicos (RAEE), garantizando la protección de la información durante todo el proceso.

10.7.3. Transferencia de información (Control 5.14)

Políticas

- La información institucional transferida mediante medios físicos o electrónicos deberá protegerse de acuerdo con su clasificación y con los controles de seguridad definidos por la Entidad.
- La transferencia de información deberá realizarse únicamente mediante mecanismos, servicios o medios autorizados por la Entidad, garantizando la confidencialidad, integridad y disponibilidad de la información durante su envío o transporte.

11. CONTROL DE ACCESO

Objetivo: Establecer los lineamientos para la gestión de identidades y el control de acceso a la información, los activos de información, los sistemas, los servicios tecnológicos y la infraestructura de la Región Metropolitana Bogotá–Cundinamarca, garantizando que únicamente las personas autorizadas accedan a los recursos de acuerdo con sus funciones, responsabilidades y necesidades del servicio.

11.1. Requisitos del negocio para el control de acceso

11.1.1. Política de control de acceso

Control 5.15 - La Entidad establecerá, implementará y mantendrá controles de acceso físico y lógico para garantizar que el acceso a la información, los activos de información, los sistemas, los servicios tecnológicos y la infraestructura institucional se otorgue únicamente a personas autorizadas, de acuerdo con las necesidades del servicio y los riesgos identificados.

Políticas

- RMBC establecerá y mantendrá controles de acceso físico y lógico para garantizar que únicamente las personas autorizadas accedan a la información, los activos de información, los sistemas, los servicios tecnológicos y la infraestructura institucional.
- Los permisos de acceso serán otorgados de acuerdo con las funciones, responsabilidades, necesidades del servicio y el principio de mínimo privilegio.
- Los accesos deberán revisarse periódicamente y actualizarse cuando se presenten cambios organizacionales, funcionales o contractuales que afecten los permisos otorgados.
- Toda asignación, modificación o revocación de accesos deberá realizarse conforme a los procedimientos definidos por la Entidad.

11.1.2. Gestión de identidades

Control 5.16 - La Entidad gestionará las identidades digitales durante todo su ciclo de vida, garantizando la creación, modificación, suspensión y eliminación de las cuentas de usuario de acuerdo con las novedades administrativas, contractuales y las necesidades del servicio.

Políticas

- La OTIC administrará el ciclo de vida de las identidades digitales de los servidores públicos, contratistas, proveedores y demás terceros autorizados.
- Cada usuario contará con una identidad única para el acceso a los servicios tecnológicos institucionales.
- La creación, modificación, suspensión y eliminación de identidades deberá realizarse con base en las novedades administrativas o contractuales informadas por las dependencias competentes.
- No se permitirá el uso de cuentas genéricas o compartidas, salvo cuando exista una necesidad técnica debidamente justificada, autorizada y controlada.

11.1.3. Información de autenticación

Control 5.17 - La información de autenticación deberá administrarse y protegerse mediante controles que garanticen su confidencialidad, integridad y uso exclusivo por parte del usuario autorizado, reduciendo el riesgo de accesos no autorizados.

Políticas

- Las credenciales de autenticación son personales, confidenciales e intransferibles y deberán ser protegidas por su titular.
- La OTIC implementará mecanismos para la gestión segura de la información de autenticación, incluyendo políticas de contraseñas, bloqueo de cuentas, restablecimiento seguro de credenciales y demás controles que resulten aplicables.
- La autenticación multifactor (MFA) será implementada para las cuentas, servicios y accesos que determine la OTIC de acuerdo con el análisis de riesgos y las capacidades tecnológicas de la Entidad.
- Toda sospecha de compromiso de las credenciales deberá reportarse inmediatamente a la Mesa de Servicio.

11.1.4. Derechos de accesos

Control 5.18 - Los derechos de acceso deberán asignarse, revisarse, modificarse y revocarse de acuerdo con las funciones del usuario, los requisitos del servicio y los principios de mínimo privilegio y necesidad de conocer, garantizando que únicamente se mantengan los accesos autorizados.

Políticas

- Los derechos de acceso deberán asignarse de acuerdo con las funciones del usuario, el principio de mínimo privilegio y la necesidad del servicio.
- Los accesos deberán contar con la autorización del responsable correspondiente antes de su asignación.

- Los derechos de acceso deberán revisarse periódicamente y modificarse, suspenderse o revocarse cuando cambien las funciones del usuario o finalice su vínculo con la Entidad.
- La OTIC mantendrá evidencia de la asignación, modificación y revocación de los derechos de acceso.

11.2. Acceso a Redes y Servicios

11.2.1. Acceso a redes y servicios

Control 8.20 - El acceso a las redes y a los servicios tecnológicos deberá administrarse mediante controles de autenticación, autorización y protección que permitan garantizar la seguridad de las comunicaciones, la disponibilidad de los servicios y la protección de la infraestructura tecnológica institucional.

Políticas

- El acceso a las redes y a los servicios tecnológicos únicamente será autorizado a los usuarios que lo requieran para el cumplimiento de sus funciones.
- La OTIC implementará mecanismos de autenticación, autorización y control de acceso para proteger las redes y los servicios tecnológicos institucionales.
- El acceso remoto y el acceso a servicios críticos deberán implementar controles de seguridad adicionales cuando así lo determine la OTIC.

11.3. Gestión de Cuentas Privilegiadas

11.3.1. Derechos de acceso privilegiado

Control 8.2 - Los accesos privilegiados deberán administrarse mediante controles reforzados que regulen su asignación, utilización, monitoreo y revocación, garantizando que únicamente el personal autorizado pueda realizar funciones de administración sobre los recursos tecnológicos de la Entidad.

Políticas

- Los privilegios administrativos únicamente serán asignados al personal autorizado y cuando exista una necesidad debidamente justificada.
- Todo acceso privilegiado deberá contar con autorización previa, quedar documentado y mantenerse bajo controles de seguimiento y trazabilidad.
- Los privilegios administrativos deberán revisarse periódicamente y revocarse cuando desaparezca la necesidad que justificó su asignación.
- Las cuentas privilegiadas deberán utilizarse exclusivamente para actividades de administración tecnológica y no para actividades de uso cotidiano.
- El personal con privilegios administrativos deberá cumplir los compromisos de confidencialidad y las políticas de seguridad de la información definidas por la Entidad.

11.4. Revisión de Accesos

11.4.1. Revisión de derechos

Control 5.18 - Los derechos de acceso a la información, los sistemas de información y los servicios tecnológicos deberán revisarse periódicamente para garantizar que permanezcan vigentes, sean apropiados para las funciones desempeñadas y se ajusten a las necesidades del servicio y a los riesgos identificados.

Políticas

- Los propietarios de la información o responsables de los sistemas apoyarán la revisión de los permisos otorgados a los usuarios bajo su responsabilidad.
- Los derechos de acceso deberán revisarse cuando se presenten cambios de cargo, funciones, dependencia, terminación del vínculo o cualquier otra situación que modifique las condiciones de acceso.
- Los permisos que no cuenten con una justificación vigente deberán modificarse o revocarse oportunamente.

11.5. Acceso a Sistemas

11.5.1. Restricción del acceso

Control 8.3 - El acceso a la información, los sistemas de información y las funcionalidades de las aplicaciones deberá restringirse de acuerdo con las políticas de control de acceso, la clasificación de la información, las funciones del usuario y los requisitos de seguridad de la Entidad

Políticas

- El acceso a la información, los sistemas de información y los servicios tecnológicos deberá restringirse de acuerdo con el rol del usuario, sus funciones y la clasificación de la información.
- La OTIC administrará los permisos de acceso bajo un modelo basado en roles, aplicando los principios de mínimo privilegio, necesidad del servicio y segregación de funciones.
- Los sistemas de información deberán implementar mecanismos que impidan el acceso no autorizado a la información y a las funcionalidades de las aplicaciones.

11.5.2. Inicio de sesión segura

Control 8.5 - Los sistemas de información y los servicios tecnológicos deberán implementar mecanismos de autenticación que permitan verificar de forma segura la identidad de los usuarios antes de conceder acceso a los recursos institucionales**.**

Políticas

- Los sistemas de información deberán implementar mecanismos de autenticación que permitan verificar la identidad de los usuarios antes de conceder acceso a los recursos tecnológicos.

- La OTIC implementará controles para registrar y monitorear los eventos de autenticación, autorización e intentos de acceso a los sistemas de información y servicios tecnológicos.
- Cuando el nivel de riesgo lo requiera, los sistemas deberán incorporar mecanismos de autenticación reforzada definidos por la OTIC.

11.5.3. Acceso al código fuente

Control 8.4 - El acceso al código fuente de los sistemas de información deberá restringirse y administrarse mediante controles que garanticen su confidencialidad, integridad, trazabilidad y uso exclusivo por personal autorizado.

Políticas

- El acceso al código fuente de los sistemas de información deberá restringirse al personal autorizado y únicamente para el desarrollo de las funciones asignadas.
- La OTIC establecerá controles para la administración, protección y trazabilidad del acceso a los repositorios de código fuente institucionales.
- El acceso al código fuente deberá registrarse, revisarse periódicamente y retirarse cuando desaparezca la necesidad que justificó su asignación.
- El código fuente institucional deberá mantenerse protegido mediante repositorios y mecanismos de control de acceso autorizados por la Entidad.

12. CRIPTOGRAFÍA

12.1. Controles Criptográficos

Objetivo: Establecer los lineamientos para el uso de controles criptográficos que permitan proteger la confidencialidad, integridad, autenticidad y disponibilidad de la información institucional durante su almacenamiento, procesamiento y transmisión.

12.1.1. Política sobre el uso de controles criptográficos

Control 8.24 - La Entidad establecerá e implementará controles criptográficos para proteger la información institucional, de acuerdo con su clasificación, los riesgos identificados, los requisitos legales y las necesidades del servicio.

Políticas

- OTIC definirá y administrará los lineamientos para el uso de mecanismos criptográficos y la gestión del ciclo de vida de las claves criptográficas.
- Los mecanismos de cifrado deberán utilizarse para proteger la información clasificada, reservada o cualquier otra información que, de acuerdo con su clasificación o análisis de riesgos, requiera protección durante su almacenamiento, procesamiento o transmisión.
- La OTIC determinará las herramientas, algoritmos y mecanismos criptográficos autorizados para la protección de la información institucional.

- Los certificados digitales, claves criptográficas, tokens y demás dispositivos utilizados para mecanismos de autenticación o cifrado deberán ser administrados y protegidos conforme a los lineamientos definidos por la Entidad.
- Los usuarios responsables de certificados digitales, tokens u otros mecanismos criptográficos deberán garantizar su adecuada custodia, evitar su préstamo, divulgación o uso por terceros no autorizados y reportar inmediatamente su pérdida, robo o compromiso de seguridad.

13. SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo: Establecer los lineamientos para proteger las personas, la información, los activos de información y la infraestructura tecnológica frente al acceso físico no autorizado, daños, pérdidas, interferencias y amenazas ambientales, garantizando la continuidad de la operación institucional.

13.1. Áreas Seguras

13.1.1. Perímetros de seguridad física

Control 7.1 La Entidad establecerá y protegerá áreas seguras mediante controles físicos y administrativos que prevengan el acceso no autorizado a la información, los activos de información y la infraestructura tecnológica.

Políticas

- La Entidad identificará y protegerá las áreas que contengan información o infraestructura crítica, de acuerdo con el análisis de riesgos.
- Las áreas seguras deberán contar con los mecanismos de protección física definidos por la Entidad, tales como controles de acceso, videovigilancia, registro de ingreso y demás medidas aplicables.
- El acceso a las áreas seguras estará restringido exclusivamente al personal autorizado.

13.1.2. Control de acceso físicos

Control 7.2 : El acceso a las áreas seguras deberá administrarse mediante controles que permitan autorizar, registrar y supervisar el ingreso de personas, equipos y demás recursos físicos.

Políticas

- El acceso a las áreas seguras se otorgará únicamente al personal autorizado conforme a sus funciones.
- Los visitantes, contratistas y proveedores deberán cumplir los controles de ingreso definidos por la Entidad y permanecer acompañados cuando accedan a áreas restringidas.

- El ingreso y salida de equipos o activos tecnológicos deberá contar con la autorización y el registro correspondiente.
- Los permisos de acceso físico deberán revisarse y actualizarse cuando cambien las funciones del usuario o finalice su vinculación con la Entidad.

13.1.3. Protección contra amenazas físicas y ambientales

Control 7.5: La Entidad implementará medidas para proteger la información, los activos de información y la infraestructura tecnológica frente a amenazas naturales, ambientales o de origen humano que puedan afectar la continuidad de la operación.

Políticas

- La Entidad implementará medidas para reducir los riesgos asociados a incendios, inundaciones, fallas eléctricas y demás amenazas físicas o ambientales.
- La OTIC velará por la protección de los centros de procesamiento de información y demás instalaciones tecnológicas bajo su responsabilidad.
- La Entidad mantendrá actualizado el Plan de Emergencias y realizará periódicamente pruebas o simulacros que fortalezcan la capacidad de respuesta frente a eventos que puedan afectar la continuidad de la operación.

13.2. Equipos

13.2.1. Ubicación y protección de los equipos

Control 7.8: Los equipos que soportan el procesamiento o almacenamiento de información deberán ubicarse y protegerse de manera que se reduzcan los riesgos de daño, pérdida, acceso no autorizado o interrupción del servicio.

Políticas

- Los equipos que procesen información clasificada o reservada deberán ubicarse en áreas con acceso restringido.
- Los equipos deberán protegerse frente a riesgos físicos y ambientales que puedan afectar su operación.
- Se prohíbe consumir alimentos, bebidas o fumar en las áreas donde se encuentren equipos que soporten el procesamiento o almacenamiento de información institucional.

13.2.2. Seguridad de cableado

Control 7.9: El cableado de energía y telecomunicaciones deberá protegerse contra daños, interferencias, interceptación o manipulaciones no autorizadas.

Políticas

- La infraestructura de cableado deberá mantenerse protegida mediante los controles físicos definidos por la Entidad.
- Las áreas de distribución eléctrica y de comunicaciones permanecerán bajo acceso restringido.

- El cableado deberá mantenerse identificado y organizado para facilitar su administración y reducir el riesgo de desconexiones o intervenciones no autorizadas.

13.2.3. Mantenimiento de equipos

Control 7.13: Los equipos tecnológicos deberán mantenerse conforme a planes de mantenimiento que garanticen su disponibilidad, integridad y funcionamiento seguro.

Políticas

- La Entidad ejecutará planes de mantenimiento preventivo y correctivo para los equipos tecnológicos.
- Las actividades de mantenimiento deberán ser realizadas por personal autorizado.
- Los usuarios no podrán modificar la configuración de los equipos sin autorización de la OTIC.
- Toda actividad de mantenimiento deberá preservar la confidencialidad, integridad y disponibilidad de la información almacenada en los equipos intervenido.

13.2.4. Equipos de usuarios desatendidos

Control 7.7: Los equipos de usuario deberán protegerse cuando permanezcan desatendidos para prevenir accesos no autorizados a la información institucional.

Políticas

- Los usuarios deberán bloquear o cerrar la sesión de trabajo al ausentarse de su puesto.
- Al finalizar la jornada deberán cerrar la sesión y apagar o asegurar los equipos conforme a los lineamientos institucionales.
- Cuando el equipo permanezca desatendido por periodos prolongados, el usuario deberá cerrar completamente la sesión o apagar el equipo, de acuerdo con las necesidades del servicio.

13.2.5. Escritorio y pantalla limpios

Control 7.7: La Entidad promoverá el uso de escritorios y pantallas limpias para reducir el riesgo de acceso no autorizado a la información en formato físico o digital.

Políticas

- La información clasificada o reservada no deberá permanecer expuesta cuando el puesto de trabajo se encuentre desatendido.
- Los documentos físicos deberán almacenarse en condiciones que garanticen su protección cuando no estén siendo utilizados.
- Los usuarios deberán retirar oportunamente los documentos enviados a impresión mediante los mecanismos de seguridad definidos por la Entidad.

- Los medios de almacenamiento removibles y los documentos que contengan información institucional deberán permanecer bajo custodia cuando no estén siendo utilizados.

14. SEGURIDAD DE LAS OPERACIONES

Objetivo: Establecer los lineamientos para la operación segura de los servicios tecnológicos, garantizando la integridad, disponibilidad y correcto funcionamiento de la infraestructura tecnológica y de los sistemas de información mediante controles operacionales documentados.

14.1. Procedimientos de Operación documentados

14.1.1. Procedimiento de operación documentados

Control 5.37: La Entidad documentará, mantendrá y actualizará los procedimientos operativos necesarios para garantizar la operación segura, consistente y controlada de los servicios tecnológicos.

Políticas

- La OTIC documentará y mantendrá actualizados los procedimientos operativos necesarios para la administración de la infraestructura tecnológica y los servicios institucionales.
- Los procedimientos deberán estar disponibles para el personal autorizado que requiera su aplicación.
- Los procedimientos operativos deberán revisarse y actualizarse cuando existan cambios tecnológicos, normativos o de operación que así lo requieran.

14.1.2. Separación de los ambientes de desarrollo, pruebas y producción

Control 8.31: La Entidad mantendrá separados los ambientes de desarrollo, pruebas y producción para reducir el riesgo de cambios no autorizados y proteger la operación de los servicios tecnológicos.

Políticas

- La OTIC garantizará la separación lógica o física de los ambientes de desarrollo, pruebas y producción, de acuerdo con la arquitectura tecnológica de la Entidad.
- Los cambios entre los ambientes de desarrollo, pruebas y producción deberán gestionarse conforme al procedimiento institucional de habilitación de cambios.
- El acceso a cada ambiente será administrado de acuerdo con el rol del usuario y las necesidades del servicio.

14.1.3. Protección contra código malicioso

Control 8.7: La Entidad implementará controles para prevenir, detectar, contener y recuperar los servicios tecnológicos frente a software malicioso que pueda afectar la seguridad de la información.

Políticas

- La OTIC implementará mecanismos de protección contra software malicioso en la infraestructura tecnológica institucional.
- Las soluciones de protección deberán mantenerse actualizadas y administradas de acuerdo con las capacidades tecnológicas de la Entidad.
- Los usuarios deberán abstenerse de instalar, ejecutar o utilizar software no autorizado que pueda comprometer la seguridad de la información.
- OTIC realizará el monitoreo de las alertas generadas por las herramientas de protección contra software malicioso y gestionará las acciones que correspondan.
- La Entidad promoverá actividades de sensibilización orientadas a prevenir los riesgos asociados al software malicioso.

14.1.4. Sincronización de relojes

Control 8.17: Los sistemas de información, dispositivos de red y demás componentes tecnológicos deberán sincronizar sus relojes con una fuente oficial de tiempo que permita garantizar la trazabilidad de los eventos y facilitar la investigación de incidentes de seguridad.

Políticas

- OTIC garantizará la sincronización de los relojes de los sistemas de información, servidores, dispositivos de red y demás componentes tecnológicos administrados por la Entidad.
- La sincronización deberá realizarse utilizando una fuente oficial de tiempo o un servicio autorizado por la Entidad.
- La configuración de sincronización deberá mantenerse durante toda la operación de los servicios tecnológicos.

14.2. Control de Software Operacional

14.2.1. Restricción para la instalación de software

Control 8.19: La instalación de software en los sistemas operacionales deberá administrarse mediante controles que garanticen la autorización, integridad y seguridad de los componentes instalados.

Políticas

- La instalación, actualización o eliminación de software en los equipos institucionales únicamente podrá ser realizada por personal autorizado o conforme a los procedimientos definidos por la OTIC.
- Se prohíbe la instalación de software no autorizado en los equipos tecnológicos de la Entidad.
- La OTIC implementará mecanismos de control que permitan restringir la instalación de software por parte de los usuarios.

- Las configuraciones de seguridad implementadas para el control del software deberán mantenerse conforme a los lineamientos institucionales.
- Toda instalación de software deberá realizarse utilizando únicamente software licenciado o autorizado por la Entidad.

14.2.2. Auditorias de sistemas de información

Control 8.34: Las actividades de auditoría que involucren acceso a los sistemas de información deberán planificarse, autorizarse y ejecutarse de manera controlada, garantizando la protección de la información y minimizando el impacto sobre la operación institucional.

Políticas

- Las auditorías que involucren acceso a sistemas de información deberán coordinarse previamente con las áreas responsables.
- Las pruebas de auditoría deberán ejecutarse procurando minimizar la afectación de la disponibilidad de los servicios tecnológicos.
- Los accesos otorgados para actividades de auditoría deberán limitarse al alcance autorizado y retirarse una vez finalicen las actividades.
- OTIC implementará mecanismos de registro, monitoreo y trazabilidad que permitan evidenciar las actividades realizadas durante las auditorías.

14.2.3. Monitoreo y seguimiento de la seguridad de la información

Control 8.16: Actividades de seguimiento - Establecer los lineamientos para el monitoreo continuo de la infraestructura tecnológica, los sistemas de información, las redes, las plataformas tecnológicas y los eventos de seguridad, con el fin de detectar oportunamente comportamientos anómalos, incidentes de seguridad y desviaciones que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Políticas

- OTIC realizará el monitoreo de la infraestructura tecnológica, redes, servicios, sistemas de información y plataformas institucionales mediante las herramientas tecnológicas disponibles.
- Se realizará seguimiento a los eventos de seguridad generados por las soluciones de seguridad implementadas, con el propósito de identificar oportunamente comportamientos anómalos, intentos de acceso no autorizado, fallas operativas e incidentes de seguridad.
- Las alertas e incidentes identificados durante el monitoreo deberán ser analizados y gestionados conforme al procedimiento institucional de gestión de incidentes de seguridad de la información.
- Los registros generados por las herramientas de monitoreo deberán conservarse de acuerdo con los tiempos de retención definidos por la Entidad y utilizarse como soporte para actividades de auditoría, análisis forense, investigaciones y mejora continua.
- OTIC realizará los ajustes necesarios para fortalecer la capacidad de detección y respuesta frente a amenazas de seguridad de la información.

14.2.4. Gestión de vulnerabilidades técnicas

Control 8.8: La Entidad gestionará las vulnerabilidades técnicas que puedan afectar sus activos de información y recursos tecnológicos.

Políticas

- La OTIC identificará, evaluará y tratará las vulnerabilidades técnicas, priorizando las acciones según la criticidad de los activos y el nivel de riesgo.

14.2.5. Gestión de la configuración

Control 8.9: La Entidad establecerá y mantendrá configuraciones seguras para sus componentes tecnológicos.

Políticas

- La OTIC controlará las configuraciones y sus modificaciones conforme al procedimiento institucional de habilitación de cambios.

14.2.6. Registro de eventos

Control 8.13: La Entidad realizará copias de respaldo para proteger la disponibilidad e integridad de la información.

Políticas

La OTIC definirá su periodicidad y retención y realizará pruebas de restauración según la criticidad de la información.

14.2.7. Gestion de la capacidad

Control 8.6: La Entidad gestionará la capacidad de sus recursos tecnológicos para garantizar la disponibilidad de los servicios.

Políticas

- La OTIC monitoreará el uso y desempeño de los recursos para prevenir afectaciones en la operación.

15. SEGURIDAD DE LAS COMUNICACIONES

Objetivo: Establecer los lineamientos para proteger la información durante su transmisión a través de las redes y servicios de comunicaciones institucionales, garantizando su confidencialidad, integridad, disponibilidad y autenticidad.

15.1. Seguridad de los Servicios de Red

15.1.1. Controles de red

Control 8.20: La Entidad implementará controles para proteger la infraestructura de red y los servicios de comunicaciones, previniendo accesos no autorizados y garantizando la seguridad de la información transmitida a través de las redes institucionales.

Políticas

- La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) administrará la infraestructura de red y los servicios de comunicaciones de la entidad.
- La infraestructura de red deberá implementar mecanismos de autenticación, control de acceso, segmentación, monitoreo y registro de eventos que permitan proteger la información y los servicios tecnológicos.
- Los dispositivos de red deberán mantenerse con configuraciones seguras, actualizaciones vigentes y controles de acceso administrados por la OTIC.
- Las comunicaciones que involucren información institucional deberán utilizar protocolos y mecanismos de protección autorizados por la Entidad.
- El acceso a la infraestructura y a los servicios de red se otorgará únicamente a usuarios autorizados, de acuerdo con sus funciones y el principio de mínimo privilegio.

15.2. Transferencia de Información

15.2.1. Mensajería electrónica

Control 5.14: La información transmitida mediante servicios de mensajería electrónica deberá protegerse utilizando los mecanismos de seguridad definidos por la Entidad, de acuerdo con su clasificación y nivel de sensibilidad.

Políticas

- El correo electrónico institucional será el medio oficial para el intercambio de información electrónica de la Entidad.
- OTIC implementará controles para proteger el servicio de correo electrónico frente a amenazas como software malicioso, phishing, suplantación de identidad, spam y fuga de información.
- Los usuarios deberán utilizar exclusivamente las cuentas institucionales para el envío o recepción de información relacionada con el ejercicio de sus funciones.
- La información clasificada o reservada deberá transmitirse utilizando los mecanismos de seguridad definidos por la Entidad.

15.2.2. Acuerdos para la transferencia de información

Control 5.14: La transferencia de información con entidades externas deberá realizarse bajo acuerdos o instrumentos que establezcan las responsabilidades y controles necesarios para proteger la información institucional.

Políticas

- Toda transferencia de información con entidades externas deberá estar soportada por el instrumento jurídico, contractual o administrativo que corresponda.

- Cuando la transferencia involucre información clasificada, reservada, datos personales o información crítica, deberán establecerse los controles de seguridad y confidencialidad aplicables.
- La Entidad mantendrá el inventario de las transferencias de información realizadas con terceros, conforme a los lineamientos institucionales.

16. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Objetivo: Establecer los lineamientos para incorporar la seguridad de la información durante la adquisición, desarrollo, implementación, mantenimiento y evolución de los sistemas de información, garantizando que los requisitos de seguridad sean considerados durante todo su ciclo de vida

16.1. Requisitos de Seguridad de los Sistemas de Información

16.1.1. Análisis y especificación de requisitos de seguridad

Control 8.26: La Entidad incorporará los requisitos de seguridad de la información en el análisis, diseño, adquisición, desarrollo, implementación y mantenimiento de los sistemas de información, de acuerdo con los riesgos identificados y las necesidades del negocio.

Políticas

- La seguridad de la información deberá incorporarse durante todo el ciclo de vida de los sistemas de información.
- Todo proyecto de adquisición, desarrollo o evolución de sistemas deberá definir y documentar los requisitos de seguridad de la información antes de su implementación.
- La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) acompañará la definición de los controles de seguridad y verificará su incorporación durante el ciclo de vida del sistema.
- Los propietarios funcionales de los sistemas aprobarán los requisitos funcionales y los perfiles de acceso asociados a los sistemas bajo su responsabilidad.

16.1.2. Seguridad de los servicios de las aplicaciones en redes públicas

Control 8.26 – Requisitos de seguridad de las aplicaciones: Los sistemas de información disponibles a través de redes públicas deberán implementar controles que protejan la información y reduzcan los riesgos de acceso no autorizado, alteración o divulgación.

Políticas

- Los sistemas expuestos a redes públicas deberán implementar mecanismos de autenticación, autorización y protección acordes con su criticidad.
- La información transmitida deberá protegerse mediante protocolos seguros y los mecanismos de seguridad definidos por la Entidad.
- El acceso remoto a los servicios tecnológicos deberá realizarse utilizando los mecanismos autorizados por la OTIC.

16.1.3. Protección de las transacciones

Control 8.26: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

Políticas

- Los sistemas deberán implementar mecanismos que garanticen la autenticación de los usuarios y el registro de las transacciones realizadas.
- La información procesada por los sistemas deberá protegerse frente a alteraciones, pérdidas o divulgaciones no autorizadas.
- Los registros de auditoría deberán conservarse conforme a los lineamientos institucionales y permitir la trazabilidad de las operaciones.

16.2. Desarrollo Seguro

16.2.1. Desarrollo seguro de software

Control 8.25: La Entidad establecerá lineamientos para garantizar que el desarrollo, mantenimiento y evolución de los sistemas de información incorporen prácticas de desarrollo seguro durante todo su ciclo de vida.

Políticas

- La adquisición, desarrollo, mantenimiento y evolución de los sistemas de información deberán realizarse conforme a los lineamientos de desarrollo seguro definidos por la Entidad.
- Los sistemas deberán someterse a pruebas funcionales y de seguridad antes de su puesta en producción y cuando se implementen cambios que puedan afectar su funcionamiento o seguridad.
- Los propietarios funcionales validarán las pruebas de aceptación y la OTIC verificará el cumplimiento de los requisitos técnicos y de seguridad antes del paso a producción.
- Los cambios a los sistemas de información deberán gestionarse conforme al procedimiento institucional de habilitación de cambios.
- Los repositorios de código fuente, componentes de desarrollo y herramientas asociadas deberán mantenerse protegidos mediante controles de acceso y trazabilidad.

17. RELACIONES CON LOS PROVEEDORES

Objetivo: Establecer los lineamientos para gestionar los riesgos de seguridad de la información asociados con los proveedores, garantizando que los bienes y servicios contratados protejan la confidencialidad, integridad y disponibilidad de la información institucional durante toda la relación contractual.

17.1. Seguridad de la Información para las Relaciones con Proveedores

17.1.1. Política de seguridad de la información para las relaciones con proveedores

Control 5.19: La Entidad establecerá y documentará los requisitos de seguridad de la información aplicables a los proveedores que tengan acceso a información, activos de información o servicios tecnológicos institucionales.

Políticas

- La Entidad incorporará los requisitos de seguridad de la información durante las etapas de planeación, contratación, ejecución y cierre de los contratos que involucren información o activos tecnológicos.
- Los riesgos asociados a los proveedores deberán identificarse y gestionarse de acuerdo con la naturaleza del servicio contratado.
- Los proveedores deberán cumplir las políticas de seguridad de la información y los lineamientos institucionales que les resulten aplicables.
- La Entidad establecerá las responsabilidades relacionadas con la protección de la información en los instrumentos jurídicos correspondientes.

17.1.2. Seguridad en los acuerdos con proveedores

Control 5.20: Los acuerdos celebrados con proveedores deberán incorporar los requisitos de seguridad de la información necesarios para proteger la información institucional y los servicios prestados.

Políticas

- Los contratos deberán incluir obligaciones relacionadas con la confidencialidad, protección de datos personales, seguridad de la información y cumplimiento de los requisitos institucionales.
- El supervisor del contrato verificará el cumplimiento de las obligaciones de seguridad de la información durante la ejecución contractual.
- Cuando la criticidad del servicio lo requiera, la Entidad podrá solicitar evidencias o verificaciones sobre la eficacia de los controles implementados por el proveedor.

17.1.3. Gestión de la Cadena de suministros de tecnología de información y comunicación

Control 5.21: La Entidad gestionará los riesgos de seguridad de la información asociados con la adquisición de productos y servicios de tecnología de la información y las comunicaciones.

Políticas

- Los proveedores de bienes o servicios tecnológicos deberán implementar controles acordes con los riesgos asociados a la cadena de suministro.

- Cuando la naturaleza del servicio lo requiera, los proveedores deberán contar con mecanismos de continuidad, recuperación y niveles de servicio acordes con la criticidad del servicio contratado.

17.1.4. Seguimiento, revisión y gestión de cambios de los servicios de los proveedores

Control 5.22: La Entidad realizará seguimiento a los servicios prestados por los proveedores para verificar el cumplimiento de los requisitos de seguridad de la información y gestionar los cambios que puedan afectar la prestación del servicio.

Políticas

- La Entidad realizará seguimiento periódico al cumplimiento de los acuerdos de niveles de servicio y de las obligaciones de seguridad de la información.
- OTIC revisará periódicamente los accesos otorgados a los proveedores sobre la infraestructura tecnológica y los sistemas de información.
- Toda modificación que pueda afectar la seguridad de la información o la prestación de los servicios deberá gestionarse conforme al procedimiento institucional de habilitación de cambios.
- Los cambios deberán evaluarse previamente considerando su impacto sobre la información, los servicios tecnológicos y la continuidad de la operación.

17.2. Uso de Servicios en la Nube

Objetivo: Establecer los lineamientos para el uso seguro de los servicios en la nube utilizados por la Región Metropolitana Bogotá–Cundinamarca, definiendo las responsabilidades de la Entidad y de los proveedores para proteger la información institucional.

Control 5.23: La Entidad implementará controles para gestionar los riesgos asociados al uso de servicios en la nube, garantizando la protección de la información durante todo el ciclo de vida del servicio.

Políticas

- La información institucional deberá almacenarse únicamente en plataformas autorizadas por la OTIC.
- Los servicios en la nube deberán implementar mecanismos de autenticación multifactor, gestión centralizada de identidades y control de acceso basado en roles, cuando sean compatibles con la plataforma utilizada.
- OTIC administrará las configuraciones de seguridad, monitoreo y auditoría de los servicios en la nube.
- La contratación de servicios en la nube deberá contemplar requisitos de seguridad, disponibilidad, continuidad del negocio, respaldo, protección de datos personales y cumplimiento normativo.

- Los incidentes de seguridad relacionados con servicios en la nube deberán gestionarse conforme al procedimiento institucional de gestión de incidentes.
- OTIC realizará evaluaciones periódicas de los riesgos y de la configuración de seguridad de las plataformas en la nube utilizadas por la Entidad.
- Cuando un servicio en la nube sea retirado o reemplazado, deberá garantizarse la recuperación o migración de la información institucional y la revocación de los accesos correspondientes.

18. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Establecer los lineamientos para la gestión de los incidentes de seguridad de la información, garantizando su identificación, reporte, evaluación, tratamiento, documentación y mejora continua, con el fin de reducir su impacto sobre la información, los servicios tecnológicos y la operación institucional.

18.1. Responsabilidades y Procedimientos

Control 5.24: La Entidad establecerá responsabilidades, procedimientos y mecanismos para preparar, gestionar y responder de manera oportuna y coordinada a los incidentes de seguridad de la información.

Políticas

- La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) coordinará la gestión de los incidentes de seguridad de la información, definiendo los procedimientos, roles, responsabilidades y canales de comunicación.
- Los servidores públicos, contratistas, proveedores y demás terceros deberán reportar y colaborar en la atención de los incidentes de seguridad de la información.
- La gestión de incidentes se realizará conforme al procedimiento institucional de gestión de incidentes de seguridad de la información.

18.2. Reporte de Eventos de Seguridad de la Información

Control 5.25: Los eventos de seguridad de la información deberán reportarse oportunamente mediante los canales definidos por la Entidad para facilitar su evaluación y tratamiento.

Políticas

- Todo evento o sospecha que pueda afectar la confidencialidad, integridad o disponibilidad de la información deberá reportarse inmediatamente a OTIC mediante los canales institucionales definidos.
- La Entidad dispondrá de mecanismos para el reporte y registro de eventos de seguridad de la información.

18.3. Evaluación de Eventos de Seguridad

Control 5.25: La Entidad evaluará los eventos reportados para determinar si corresponden a incidentes de seguridad de la información y definir las acciones de respuesta apropiadas.

Políticas

- OTIC evaluará los eventos reportados para determinar su impacto, criticidad y clasificación.
- Los incidentes de seguridad serán atendidos de acuerdo con su nivel de impacto y prioridad.
- Cuando la naturaleza del incidente lo requiera, se realizará el escalamiento a las dependencias o autoridades competentes.

18.4. Aprendizaje de los Incidentes de Seguridad de la Información

Control 5.27: La información obtenida durante la gestión de los incidentes deberá utilizarse para fortalecer los controles de seguridad de la información y reducir la probabilidad de ocurrencia de incidentes similares.

Políticas

- Los incidentes deberán documentarse y analizarse para identificar sus causas y oportunidades de mejora.
- Las lecciones aprendidas deberán incorporarse, cuando corresponda, a los procesos, procedimientos, controles y actividades de sensibilización de la Entidad.

18.5. Recolección y Preservación de Evidencias

Control 5.28: La Entidad establecerá mecanismos para la identificación, recolección, preservación y custodia de las evidencias relacionadas con incidentes de seguridad de la información, garantizando su integridad y disponibilidad.

Políticas

- La recolección y preservación de evidencias deberá realizarse de forma que garantice su integridad, autenticidad y trazabilidad.
- Las evidencias deberán conservarse cuando puedan ser requeridas para investigaciones, procesos administrativos, disciplinarios o judiciales.
- El acceso a las evidencias estará restringido al personal autorizado.

19. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

Objetivo: Establecer los lineamientos para garantizar la continuidad de la seguridad de la información durante situaciones de crisis, contingencia o desastre, asegurando la disponibilidad de los procesos, los servicios tecnológicos y los activos de información críticos de la Entidad.

19.1. Continuidad de la Seguridad de la información

19.1.1. Planificación de la continuidad de la seguridad de la información

Control 5.29: La Entidad establecerá los requisitos y estrategias necesarias para mantener la seguridad de la información durante situaciones que afecten la continuidad de la operación, de acuerdo con el análisis de riesgos y el impacto al negocio.

Políticas

- La continuidad de la seguridad de la información deberá incorporarse en los procesos de continuidad del negocio y recuperación de desastres de la Entidad.
- La planificación de la continuidad deberá fundamentarse en el análisis de impacto al negocio, la gestión de riesgos y la identificación de los procesos y servicios críticos.
- La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), en coordinación con las dependencias competentes, definirá las estrategias necesarias para garantizar la recuperación de los servicios tecnológicos y la protección de la información institucional.

19.1.2. Implementación de la continuidad de la seguridad de la información

Control 5.30: La Entidad implementará y mantendrá las capacidades tecnológicas necesarias para soportar la continuidad del negocio y la recuperación de los servicios tecnológicos durante situaciones adversas.

Políticas

- OTIC implementará y mantendrá el Plan de Recuperación ante Desastres (DRP) y los demás mecanismos tecnológicos requeridos para la continuidad de los servicios críticos.
- La Entidad mantendrá documentados los procedimientos de recuperación tecnológica y retorno a la operación normal.

19.1.3. Verificación, revisión y mejora de la continuidad

Control 5.30: La Entidad verificará periódicamente la eficacia de los planes, procedimientos y controles implementados para garantizar la continuidad de la seguridad de la información.

Políticas

- La Entidad realizará pruebas, simulacros y ejercicios periódicos para verificar la eficacia de los planes de continuidad y recuperación.
- Los resultados obtenidos deberán documentarse y utilizarse para fortalecer los planes, procedimientos y controles implementados.
- OTIC realizará seguimiento a las acciones de mejora derivadas de las pruebas y ejercicios ejecutados.

19.2. Redundancia

19.2.1. Disponibilidad de las instalaciones de procesamiento de información

Control 8.14: La Entidad implementará mecanismos de redundancia que permitan mantener la disponibilidad de los servicios tecnológicos y reducir el impacto de las interrupciones sobre la operación institucional.

Políticas

- La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) implementará mecanismos de redundancia para la infraestructura tecnológica y los servicios críticos, de acuerdo con las necesidades de disponibilidad de la Entidad.
- La arquitectura tecnológica deberá incorporar mecanismos de alta disponibilidad, respaldo y recuperación acordes con la criticidad de los servicios.
- Los mecanismos de redundancia deberán mantenerse, revisarse y probarse periódicamente para verificar su eficacia.
- OTIC evaluará periódicamente la capacidad de recuperación de la infraestructura tecnológica y establecerá las acciones de mejora que resulten necesarias.

20. CUMPLIMIENTO

21.

Objetivo: Establecer los lineamientos para garantizar el cumplimiento de los requisitos legales, regulatorios, contractuales e institucionales relacionados con la seguridad de la información, así como verificar la eficacia de los controles implementados dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

21.1. Cumplimiento de Requisitos Legales y Contractuales

21.1.1. Identificación de requisitos legales, regulatorios y contractuales

Control 5.31: La Entidad identificará, documentará, mantendrá actualizados y dará cumplimiento a los requisitos legales, regulatorios, estatutarios y contractuales aplicables a la seguridad de la información.

Políticas

- La Entidad mantendrá actualizado el normograma institucional con los requisitos aplicables en materia de seguridad de la información, protección de datos personales, gobierno digital y demás disposiciones relacionadas.
- Los servidores públicos, contratistas, proveedores y terceros deberán cumplir los requisitos legales, contractuales y las políticas institucionales que les resulten aplicables.

21.1.2. Derechos de propiedad intelectual

Control 5.32: La Entidad protegerá los derechos de propiedad intelectual y garantizará el uso legal de software, información y demás activos protegidos por la legislación vigente.

Políticas

- La Entidad utilizará únicamente software debidamente licenciado o autorizado.
- La OTIC realizará el control del software instalado en la infraestructura tecnológica institucional.
- Los contratos deberán incorporar las cláusulas relacionadas con propiedad intelectual y derechos de autor cuando corresponda.

21.1.3. Protección de registros

Control 5.33: La Entidad protegerá los registros institucionales contra pérdida, alteración, destrucción, acceso o divulgación no autorizada, conforme a los requisitos legales y las necesidades del negocio.

Políticas

- Los registros institucionales deberán clasificarse y protegerse de acuerdo con los lineamientos de gestión documental y seguridad de la información.
- La Gestión Documental administrará los tiempos de conservación y disposición final conforme a las Tablas de Retención Documental.
- Los responsables de los procesos garantizarán la protección y disponibilidad de los registros bajo su responsabilidad.

21.1.4. Privacidad y protección de información de datos personales

Control 5.34: La Entidad implementará controles para garantizar el tratamiento adecuado de los datos personales, conforme a la legislación vigente y a los principios de privacidad aplicables.

Políticas

- La Entidad mantendrá actualizada la Política de Tratamiento de Datos Personales.
- El acceso a los datos personales estará restringido al personal autorizado y conforme a la finalidad para la cual fueron recolectados.
- Las bases de datos personales deberán registrarse y mantenerse actualizadas ante la Superintendencia de Industria y Comercio.

21.1.5. Cumplimiento de controles criptográficos

Control 8.24: La Entidad utilizará mecanismos criptográficos conforme a la legislación vigente y a los lineamientos institucionales para proteger la información.

Políticas

- Los controles criptográficos deberán implementarse conforme a los lineamientos definidos por la Entidad y la normatividad vigente.
- La utilización de mecanismos criptográficos deberá cumplir los requisitos legales y técnicos aplicables.

21.2. Verificación del Cumplimiento

21.2.1. Revisión independiente de la seguridad de la información

Control 5.35: La Entidad realizará revisiones independientes para verificar que el Sistema de Gestión de Seguridad de la Información se implemente y opere conforme a las políticas y requisitos establecidos.

Políticas

- La Entidad realizará auditorías internas y revisiones periódicas del SGSI.
- Los resultados de las auditorías deberán generar acciones de mejora cuando corresponda.

21.2.2. Cumplimiento de las políticas y normas de seguridad

Control 5.36: La Entidad verificará periódicamente el cumplimiento de las políticas, procedimientos y controles de seguridad de la información.

Políticas

- Los responsables de los procesos verificarán el cumplimiento de las políticas de seguridad de la información dentro de su ámbito de responsabilidad.
- Los incumplimientos identificados deberán reportarse mediante los mecanismos institucionales establecidos para su análisis y tratamiento.
- La Entidad realizará seguimiento a las acciones correctivas y de mejora derivadas de las verificaciones realizadas.

17. CONTROL DE DOCUMENTOS

Versión	Fecha de aprobación	Descripción de la modificación
1	08-09-2026	Creación del documento

ELABORÓ	Brahiam Alirio Cruz Aleman Martha Lucia González Maldonado	Contratistas	Oficina de las Tecnologías de la Información y las comunicaciones
REVISÓ	Silvana Lorena Chaves Patiño	Contratista	Oficina Asesora de Planeación Institucional
APROBÓ	Liliana Morales	Jefe	Oficina de las Tecnologías de la Información y las comunicaciones
FECHA DE APROBACIÓN	*Comité Institucional De Gestión Y Desempeño*		