Política

Somos epicentro
global de CTi+E.

Seguridad y privacidad de la información

Código: PL-ADF-TI-001
Versión 1

ruta n MEDELLÍN
CENTRO DE INNOVACIÓN Y NEGOCIOS

Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

Hoja de aprobación

ELABORÓ	**Javier Dario Arcila Calderón** Profesional de infraestructura TI	**Firma** Javier Arcila
ELABORÓ	**Jaiber Ortíz Valdés** Profesional de infraestructura TI	**Firma** Jaiber Ortiz
REVISÓ	**Sebastián Marín Loaiza** Líder de infraestructura y TI	**Firma**
REVISÓ	**Virmar Yessid David Valle** Subdirector administrativo y financiero	**Firma**
REVISÓ	**Alexander Cuspoca Chaparro** Profesional de excelencia y sostenibilidad	**Firma** Alexander C.
APROBÓ	**Carolina Londoño Peláez** Directora ejecutiva	**Firma** Carolina Londoño P.

Hoja de control de cambios

VERSIÓN	DESCRIPCIÓN / CONTROL DE CAMBIOS	FECHA DE APROBACIÓN
1	Documento original	Ver fecha de firma electrónica

Índice

1. OBJETIVO

Establecer el marco normativo de obligatorio cumplimiento para la protección de la información y los activos tecnológicos de la Corporación Ruta N, asegurando la confidencialidad, integridad y disponibilidad de la información a lo largo de todo su ciclo de vida.

Esta política define los principios, responsabilidades y lineamientos que orientan la gestión de los riesgos de seguridad y privacidad de la información en la Corporación Ruta N , promoviendo una cultura de protección y uso responsable de la tecnología por parte de todos los actores que interactúan con los activos de información institucionales.

2. ALCANCE

Esta política es el instrumento de más alto nivel en materia de seguridad y privacidad de la información de la Corporación Ruta N. Todos los documentos, normas, procedimientos y controles que se desarrollen en la Corporación deberán estar subordinados y alineados a lo aquí dispuesto.

Su cumplimiento es obligatorio para:

Personas: todos los colaboradores, directivos, contratistas, proveedores, aliados, practicantes, voluntarios y cualquier tercero que, en virtud de una relación con la Corporación, tenga acceso a sus activos de información.

Activos de información: toda la información de la Corporación, independientemente de su formato (físico, digital, magnético u óptico), medio de transmisión, ubicación geográfica o régimen de propiedad, incluyendo activos propios, arrendados, de terceros, en la nube o en dispositivos personales.

Infraestructura y servicios tecnológicos: todas las sedes, redes, sistemas, aplicaciones, plataformas y servicios tecnológicos propios o de terceros utilizados para el procesamiento, almacenamiento, transmisión o eliminación segura de información de la Corporación.

El periodo de aplicación de esta política comprende desde el momento en que una persona o entidad establece una relación con la Corporación Ruta N, hasta que todos sus accesos, activos e información hayan sido formalmente reintegrados o revocados. No se admitirán exclusiones sin una excepción formalmente aprobada por la instancia competente.

3. REFERENCIAS

ISO/IEC 27001: norma internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la gestión de riesgos.

NIST CSF (Cybersecurity Framework): marco de referencia desarrollado por el National Institute of Standards and Technology de Estados Unidos, que orienta la gestión del riesgo en ciberseguridad a través de cinco funciones: identificar, proteger, detectar, responder y recuperar.

Ley 1581 de 2012: normativa colombiana que establece el régimen general de protección de datos personales, definiendo principios, derechos y obligaciones para el tratamiento adecuado de la información personal.

Ley 1273 de 2009: ley colombiana que tipifica los delitos informáticos y protege la confidencialidad, integridad y disponibilidad de los datos y sistemas de información.

Decreto 1078 de 2015: decreto único reglamentario del sector TIC en Colombia, que compila y regula disposiciones relacionadas con la gestión de tecnologías de la información y las comunicaciones en el país.

Guía MSPI MinTIC: lineamiento del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia que orienta la implementación del Modelo de Seguridad y Privacidad de la Información en entidades públicas.

4. GLOSARIO

Activo de Información: todo elemento que tiene valor para la Corporación Ruta N y que contiene, procesa, almacena, transmite o soporta información. Incluye datos, documentos, bases de datos, aplicaciones, sistemas de información, equipos tecnológicos, servicios en la nube, medios físicos, conocimiento institucional y recursos humanos asociados a la gestión de la información.

Amenaza: cualquier evento, situación, actor o acción con capacidad de causar daño, afectar la operación o comprometer la confidencialidad, integridad o disponibilidad de los activos de información de la Corporación. Las amenazas pueden ser internas o externas, accidentales o intencionales.

ANS (Acuerdo de Nivel de Servicio): documento formal que establece los compromisos de tiempo, calidad y condiciones bajo los cuales el proceso de TI presta sus servicios a los usuarios internos y externos de la Corporación. Define, entre otros, los tiempos máximos de atención y resolución según el nivel de criticidad del requerimiento o incidente.

BitLocker: herramienta de cifrado de disco integrada en sistemas operativos Windows, utilizada para proteger la información almacenada en equipos corporativos mediante el cifrado completo del disco.

BYOD: acrónimo de Bring Your Own Device (Trae tu propio dispositivo). Práctica que permite a colaboradores y contratistas utilizar sus dispositivos personales para acceder a recursos corporativos, sujeto a las condiciones definidas en esta política.

Ciberseguridad: conjunto de prácticas y medidas para proteger sistemas, redes e información frente a ataques digitales.

Cifrado de Disco: mecanismo de seguridad que protege toda la información almacenada en un disco (disco duro o SSD) convirtiéndola en datos ilegibles mediante algoritmos de cifrado. En la Corporación se implementa mediante BitLocker para equipos Windows y FileVault para equipos macOS.

Clasificación de la Información: proceso mediante el cual la información es categorizada según su nivel de sensibilidad, criticidad y necesidad de protección, con el fin de definir los controles adecuados para su acceso, uso, almacenamiento, transmisión y disposición final.

Compromiso de Seguridad: situación en la que un dispositivo o sistema presenta indicios de haber sido vulnerado, afectado por malware, manipulado sin autorización o expuesto a actividades que ponen en riesgo la información o la infraestructura de la Corporación.

Confianza Cero: modelo de seguridad que asume que ningún usuario o dispositivo es confiable por defecto, exigiendo verificación continua para el acceso a recursos.

Confidencialidad: propiedad que garantiza que la información sea accesible únicamente a personas autorizadas.

Cuenta Genérica: identidad digital que no está asociada directamente a una persona natural específica, utilizada para funciones o servicios compartidos dentro de la Corporación.

Cuenta Nombrada: identidad digital asignada de manera exclusiva a una persona natural, utilizada para el acceso a los sistemas de información, servicios tecnológicos y plataformas corporativas de Ruta N.

Datos Personales: información vinculada o que pueda asociarse a una persona natural identificada o identificable, conforme a lo establecido en la Ley 1581 de 2012.

Disponibilidad: propiedad que garantiza que la información y los sistemas estén accesibles cuando sean requeridos.

Disponibilidad Operativa: capacidad de los sistemas, servicios tecnológicos, plataformas e infraestructura de mantenerse accesibles y funcionando adecuadamente para soportar la operación de la Corporación cuando sean requeridos por los usuarios autorizados.

EDR: acrónimo de Endpoint Detection and Response. Herramienta de ciberseguridad diseñada para monitorear, detectar y responder a amenazas en los dispositivos de una organización.

Hash: 2864bbc1b0ff885ae009be09c374c472a3d41a42d86d32491d98fc31074b268b

FileVault: herramienta de cifrado de disco integrada en sistemas operativos macOS, utilizada para proteger la información almacenada en equipos corporativos Apple mediante el cifrado completo del disco.

Framework: marco de trabajo estructurado que ofrece lineamientos, buenas prácticas o herramientas reutilizables para el desarrollo de tareas complejas, como gestión de proyectos, desarrollo de software o implementación de controles de seguridad.

Hotspot: punto de acceso a Internet proporcionado por un dispositivo que comparte su conexión mediante Wi-Fi.

Incidente de Seguridad: evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información.

Integridad: propiedad que asegura que la información es exacta, completa y no ha sido modificada de forma indebida.

MFA: acrónimo de Multi-Factor Authentication (Autenticación Multifactor). Medida de seguridad que exige a los usuarios proporcionar dos o más formas de verificación para acceder a una cuenta o aplicación.

Mínimo Privilegio: principio según el cual una persona solo debe tener los accesos estrictamente necesarios para el desempeño de su trabajo.

OneDrive: servicio de almacenamiento en la nube de Microsoft, integrado al ecosistema Microsoft 365, utilizado en la Corporación para el almacenamiento, sincronización y compartición de archivos de forma segura.

Portal Cautivo: mecanismo de control de acceso a una red Wi-Fi que redirige al usuario a una página de autenticación o aceptación de condiciones de uso antes de permitirle navegar en internet. Utilizado en redes de visitantes y espacios de coworking de la Corporación.

Repetidor: dispositivo que amplifica y retransmite la señal Wi-Fi para extender su alcance dentro de una red.

Riesgo: posibilidad de que una amenaza aproveche una vulnerabilidad y genere un impacto negativo sobre la confidencialidad, integridad o disponibilidad de la información, afectando los objetivos, procesos, operaciones o reputación de la Corporación.

Router: equipo que conecta y dirige el tráfico entre redes.

Segmentación de Red: división de una red en segmentos independientes con el fin de limitar accesos no autorizados y reducir el impacto de posibles incidentes de seguridad.

SharePoint: plataforma de colaboración y gestión documental de Microsoft, integrada al ecosistema Microsoft 365, utilizada en la Corporación para el almacenamiento, organización y gestión de documentos e información institucional.

SSID: acrónimo de Service Set Identifier (Identificador de Conjunto de Servicios). Nombre técnico que identifica una red Wi-Fi.

VLAN: acrónimo de Virtual Local Area Network (Red de Área Local Virtual). Red lógica que divide una red física en múltiples redes independientes para mejorar la segmentación y el control del tráfico.

VPN: acrónimo de Virtual Private Network (Red Privada Virtual). Servicio que cifra la conexión a internet y protege la dirección IP del usuario, creando un túnel seguro entre su dispositivo y la red de destino.

Vulnerabilidad: debilidad, falla o ausencia de controles en un sistema, proceso, dispositivo, infraestructura o procedimiento, que puede ser explotada por una amenaza para comprometer la seguridad de la información

5. RESPONSABILIDADES

Dirección Ejecutiva

- Aprobar la presente Política de Seguridad y Privacidad de la Información, así como sus actualizaciones y modificaciones.
- Respaldar y promover las iniciativas estratégicas relacionadas con la seguridad y privacidad de la información en la Corporación Ruta N.
- Velar por el cumplimiento de la política en todos los niveles y procesos de la Corporación Ruta N.
- Fomentar una cultura organizacional orientada a la protección de la información y al uso seguro de los recursos tecnológicos.
- Garantizar la asignación de recursos necesarios para la implementación y mejora continua de los controles de seguridad de la información.

Directores, subdirectores y lideres

- Garantizar que los colaboradores, contratistas y terceros a su cargo conozcan, comprendan y cumplan la presente política y los lineamientos asociados.
- Autorizar formalmente los accesos a los activos de información y servicios tecnológicos de acuerdo con las funciones y necesidades operativas de cada usuario.
- Revisar y validar periódicamente los accesos, permisos y privilegios asignados a los usuarios bajo su responsabilidad.
- Gestionar y monitorear los riesgos de seguridad de la información asociados a sus procesos, conforme a la matriz de riesgos institucional.
- Reportar oportunamente al proceso de TI cualquier situación que pueda comprometer la seguridad de la información o el cumplimiento de esta política.

Proceso de TI

- Definir, implementar y mantener controles de seguridad técnicos, tecnológicos y administrativos que permitan el cumplimiento de la presente política.
- Administrar de forma segura los accesos, plataformas, redes, sistemas de información y demás recursos tecnológicos de la Corporación.
- Gestionar los incidentes y eventos de seguridad de la información, incluyendo su identificación, análisis, contención, recuperación y documentación.
- Monitorear de manera continua las amenazas, vulnerabilidades y riesgos que puedan afectar la infraestructura tecnológica y los activos de información.
- Diseñar, coordinar y apoyar actividades de capacitación, sensibilización y fortalecimiento de la cultura de seguridad de la información.
- Mantener actualizado al personal de apoyo tecnológico en materia de seguridad de la información y ciberseguridad, promoviendo la mejora continua de políticas, procedimientos y controles.
- Implementar mecanismos de seguimiento y monitoreo que permitan detectar accesos no autorizados, actividades inusuales o posibles incidentes de seguridad.

Colaboradores, Contratistas y Terceros

- Cumplir las disposiciones establecidas en la presente política, así como los lineamientos, procedimientos y controles asociados a la seguridad de la información.
- Proteger las credenciales, dispositivos, accesos y activos de información puestos bajo su responsabilidad.
- Reportar de manera inmediata cualquier incidente, evento sospechoso, vulnerabilidad o incumplimiento relacionado con la seguridad de la información.
- Utilizar los recursos tecnológicos y la información corporativa únicamente para fines autorizados y relacionados con sus funciones o actividades contractuales.
- Participar en las actividades de formación, capacitación y sensibilización definidas por la Corporación en materia de seguridad y privacidad de la información.

Dirección de Control Interno

- Evaluar periódicamente la efectividad, pertinencia y cumplimiento de los controles establecidos en el marco de la presente política.
- Incluir dentro de su plan anual de auditoría la verificación del cumplimiento de los lineamientos normativos, técnicos y organizacionales relacionados con la privacidad y seguridad de la información.
- Realizar seguimiento a los hallazgos, oportunidades de mejora y planes de acción derivados de auditorías o evaluaciones relacionadas con seguridad de la información.
- Emitir recomendaciones orientadas al fortalecimiento del sistema de control interno y de la gestión de riesgos asociados a la seguridad de la información.

6. LINEAMIENTOS

6.1. Principios de seguridad de la información:

Los principios de seguridad de la información establecen las bases para la protección de los activos de información de la Corporación Ruta N y constituyen el marco general sobre el cual se desarrollan las normas, lineamientos y controles en esta materia. La presente política se define como el instrumento rector y de mayor jerarquía en seguridad y privacidad de la información, del cual se derivan las prácticas, procedimientos y controles aplicables en toda la Corporación.

En coherencia con su rol institucional, la Corporación Ruta N establece y desarrolla esta política como parte de sus buenas prácticas organizacionales, con el fin de garantizar que la información sea gestionada de manera segura, confiable y disponible, fortaleciendo una cultura de protección de la información y uso responsable de la tecnología.

La Corporación Ruta N adopta los siguientes principios como fundamento obligatorio de todas las decisiones, controles y conductas relacionadas con la seguridad y privacidad de la información:

6.1.1. Confidencialidad

Garantizar que la información sea accesible únicamente para personas, procesos o sistemas debidamente autorizados, de acuerdo con sus funciones y responsabilidades.

El acceso a la información se otorgará bajo los principios de mínimo privilegio y necesidad de conocer, considerando los diferentes perfiles de usuarios, tales como empleados, contratistas, aliados y terceros. Cualquier acceso no autorizado, divulgación indebida o uso inapropiado de la información será considerado un incumplimiento de la presente política.

6.1.2. Integridad

Asegurar que la información se mantenga completa, exacta, consistente y protegida frente a modificaciones no autorizadas, intencionales o accidentales, durante todo su ciclo de vida.

La Corporación deberá implementar mecanismos que permitan prevenir, detectar y corregir alteraciones indebidas de la información, garantizando que los datos utilizados para la toma de decisiones, la operación institucional y la relación con terceros sean confiables y trazables.

6.1.3. Disponibilidad

La información, los sistemas de información y los servicios tecnológicos deberán mantenerse disponibles y accesibles cuando la operación de la Corporación lo requiera, de acuerdo con los niveles de servicio definidos institucionalmente.

La organización establecerá medidas preventivas, correctivas y de contingencia orientadas a reducir el impacto de incidentes que puedan afectar la continuidad de los servicios, considerando amenazas tecnológicas, operativas, internas y externas.

6.1.4. Gestión del Riesgo

La seguridad de la información en la Corporación Ruta N se gestionará bajo un enfoque basado en riesgos, reconociendo que no todos los activos, procesos o escenarios presentan el mismo nivel de criticidad.

Los controles de seguridad serán definidos, priorizados e implementados con base en la identificación, análisis, evaluación y tratamiento de riesgos, teniendo en cuenta la naturaleza de la información, el contexto operativo de la organización y la participación de terceros, tales como contratistas, aliados y usuarios.

6.1.5. Confianza Cero

La Corporación Ruta N adopta el principio de Confianza Cero, según el cual ningún usuario, dispositivo, red o sistema será considerado confiable por defecto, independientemente de su ubicación o relación con la organización.

Todo acceso a los recursos de información deberá ser autenticado, autorizado y monitoreado de manera continua, considerando los diferentes niveles de control existentes sobre los dispositivos y entornos desde los cuales se accede a la infraestructura tecnológica corporativa.

6.1.6. Protección de Datos Personales

Los datos personales serán protegidos conforme a la legislación vigente y la política de tratamiento de datos de la Corporación Ruta N, garantizando su confidencialidad, integridad y disponibilidad.

El tratamiento de los datos personales se realizará únicamente para fines legítimos, autorizados y necesarios, mediante la aplicación de medidas técnicas, administrativas y organizacionales orientadas a prevenir su uso indebido, acceso no autorizado, pérdida, alteración o divulgación.

6.2. Marcos de referencia

La Política de Seguridad y Privacidad de la Información de la Corporación Ruta N se fundamenta en marcos de referencia y estándares internacionales ampliamente reconocidos, los cuales proporcionan principios, lineamientos y buenas prácticas para la gestión de la privacidad y seguridad de la información.

Estos marcos son adoptados como referentes estratégicos para orientar la toma de decisiones, priorizar la implementación de controles de seguridad y gestionar los riesgos de manera coherente con la naturaleza, el tamaño y el modelo operativo de la Corporación Ruta N. Su aplicación se

desarrolla de manera gradual y proporcional, considerando la interacción de empleados, contratistas, aliados y usuarios, así como los diferentes niveles de control existentes sobre la infraestructura tecnológica.

Los marcos de referencia adoptados son los siguientes:

6.2.1. Sistema de Gestión de Seguridad de la Información (SGSI)- ISO/IEC 27001

La norma ISO/IEC 27001 establece un enfoque sistemático para la protección de la información mediante la identificación, análisis, evaluación y tratamiento de riesgos, garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

Este estándar sirve como base para:

- Definir el enfoque de gestión de riesgos de seguridad de la información.
- Establecer principios, roles y responsabilidades organizacionales.
- Implementar controles orientados a la protección de la información.
- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), alineada con los objetivos estratégicos de la Corporación.

La referencia a la norma ISO/IEC 27001 no implica la existencia de una certificación formal, sino la adopción de sus principios y buenas prácticas como guía para el fortalecimiento progresivo de la seguridad de la información en la Corporación.

6.2.2. NIST Cybersecurity Framework (CSF)

El NIST Cybersecurity Framework (CSF) complementa el enfoque de ISO/IEC 27001 al proporcionar una estructura práctica y flexible para la gestión de riesgos de ciberseguridad, organizada en las funciones de Identificar, Proteger, Detectar, Responder y Recuperar.

Este marco permite:

- Facilitar la comprensión, gestión y comunicación de los riesgos de ciberseguridad.
- Priorizar controles de seguridad en entornos con múltiples actores, dispositivos y niveles de acceso.
- Fortalecer las capacidades de prevención, detección, respuesta y recuperación frente a incidentes de seguridad.
- Mejorar la resiliencia tecnológica y operativa de la Corporación frente a amenazas internas y externas.

La adopción de estos marcos de referencia no implica una certificación obligatoria; sin embargo, sí establece el compromiso institucional de implementar y mantener controles alineados con sus principios y buenas prácticas, en proporción al nivel de riesgo, capacidad operativa y necesidades de la Corporación Ruta N.

6.3. Gestión de accesos y uso aceptable.

La gestión de accesos en la Corporación Ruta N deberá regirse por los siguientes lineamientos:

- Todo acceso a los activos de información deberá contar con autorización previa y formal por parte del responsable del activo y del líder del área solicitante, salvo en aquellos casos en los que el responsable del área tenga delegada directamente la administración de dichos permisos, como ocurre con algunas plataformas colaborativas, entre ellas SharePoint.
- Las cuentas de usuario son personales, intransferibles e indelegables. Su uso por parte de terceros únicamente podrá realizarse con autorización previa y expresa de la Dirección, Secretaría General o Subdirección correspondiente.
- Las cuentas nombradas deberán utilizarse exclusivamente para el desarrollo de actividades laborales autorizadas. Se prohíbe expresamente su uso para fines personales o actividades ajenas a las funciones asignadas.
- Toda cuenta genérica deberá contar con un responsable formalmente designado, quien asumirá la responsabilidad sobre su administración, uso adecuado y cualquier incidente de seguridad de la información asociado a esta.
- No se permitirá la creación ni la continuidad de cuentas genéricas que no tengan un responsable asignado y debidamente identificado.
- La Corporación Ruta N mantendrá un inventario centralizado, actualizado y controlado de todas las cuentas genéricas, garantizando su adecuada administración y trazabilidad.
- Las cuentas genéricas deberán utilizarse únicamente para los fines operativos previamente autorizados por la Corporación.
- Todas las cuentas, tanto nombradas como genéricas, deberán cumplir los controles mínimos de seguridad definidos por la Corporación, incluyendo el uso de contraseñas robustas y la autenticación multifactor (MFA).
- Se prohíbe compartir credenciales, así como permitir el uso de sesiones activas por parte de terceros no autorizados.
- Los accesos y privilegios asignados deberán ser revisados, validados y recertificados por los líderes de área, como mínimo, cada seis (6) meses.
- Ante la terminación de cualquier vínculo laboral, contractual o institucional, la revocación de accesos deberá ejecutarse de manera inmediata y prioritaria, respetando los tiempos máximos establecidos en los Acuerdos de Nivel de Servicio (ANS) definidos por el proceso de TI.
- Todos los accesos a recursos corporativos deberán implementar autenticación multifactor (MFA), siempre que las capacidades técnicas de la aplicación o plataforma lo permitan.
- El uso de los recursos tecnológicos de la Corporación Ruta N deberá realizarse exclusivamente para fines laborales, institucionales y lícitos, en cumplimiento de las disposiciones internas y la normativa aplicable

6.4. Gestión de plataformas, dispositivos y accesos asociados.

La Corporación Ruta N establecerá, implementará y mantendrá controles de seguridad técnicos, tecnológicos y administrativos para la gestión de las plataformas tecnológicas, los dispositivos y los accesos asociados, con el propósito de proteger los activos de información y reducir los riesgos relacionados con el acceso no autorizado, la pérdida, alteración, divulgación indebida o uso inadecuado de la información.

La gestión de plataformas, dispositivos y accesos asociados comprende los controles aplicables a:

- Dispositivos corporativos asignados a colaboradores y usuarios vinculados a la Corporación.
- Dispositivos personales utilizados por contratistas o terceros bajo el esquema BYOD (Bring Your Own Device).
- Dispositivos utilizados por invitados, visitantes o usuarios temporales que accedan a la infraestructura tecnológica de la Corporación.

Los controles definidos en esta política serán de obligatorio cumplimiento para todos los usuarios que interactúen con la infraestructura tecnológica y los activos de información de la Corporación. Asimismo, podrán ser ajustados, fortalecidos o complementados de acuerdo con las necesidades operativas, el contexto de riesgo, los cambios tecnológicos y la evolución de las amenazas de seguridad de la información y ciberseguridad.

Cualquier actualización o modificación de dichos controles deberá ser formalmente documentada, aprobada, publicada y comunicada por los medios institucionales definidos por la Corporación.

6.4.1. Gestión de acceso vinculados y seguridad en dispositivos corporativos

1. Todo dispositivo provisto por la Corporación Ruta N deberá estar incorporado al dominio corporativo y permanecer bajo la administración y control del proceso de TI.

2. El acceso a la red corporativa desde dispositivos institucionales únicamente se permitirá mediante el SSID corporativo autorizado dentro de las instalaciones de la Corporación o a través de la VPN corporativa para esquemas de trabajo remoto, previa autorización del jefe inmediato o del responsable correspondiente.

3. Los dispositivos corporativos deberán contar, como mínimo, con los siguientes controles de seguridad:

    - Sistema operativo con soporte y actualizaciones vigentes.
    - Solución de seguridad Endpoint Detection and Response (EDR) instalada, activa y actualizada.
    - Firewall del sistema operativo habilitado y operativo.
    - Cifrado de disco obligatorio mediante herramientas autorizadas por la Corporación, tales como BitLocker o FileVault.
    - Bloqueo automático de sesión por inactividad en un tiempo máximo de cinco (5) minutos.

4. Las contraseñas utilizadas en los dispositivos corporativos deberán cumplir con los lineamientos de seguridad definidos por la Corporación, incluyendo una longitud mínima de ocho (8) caracteres y criterios de complejidad que contemplen mayúsculas, minúsculas, números y caracteres especiales. Asimismo, deberán renovarse periódicamente conforme a los tiempos establecidos institucionalmente, los cuales no podrán superar ciento veinte (120) días.

5. Se prohíbe almacenar información clasificada como sensible o confidencial en discos locales o medios no autorizados, salvo aprobación expresa del responsable del activo de información. Para el almacenamiento, gestión y compartición de información institucional deberán utilizarse únicamente las plataformas autorizadas por la Corporación, tales como SharePoint y OneDrive.

6. Los usuarios de dispositivos corporativos serán responsables de:

   - Custodiar adecuadamente los equipos asignados y evitar su uso por parte de terceros no autorizados.
   - Reportar al proceso de TI la pérdida, robo o extravío del dispositivo en un plazo máximo de dos (2) horas hábiles desde que tengan conocimiento del evento.
   - Informar oportunamente cualquier comportamiento inusual, incidente o sospecha de compromiso de seguridad relacionado con el dispositivo.

7. Se prohíbe el uso de los equipos y recursos tecnológicos de la Corporación para actividades personales, ilícitas o ajenas a las funciones y responsabilidades asignadas.

8. El acceso a dispositivos corporativos, servicios VPN, correo electrónico institucional y demás recursos tecnológicos deberá realizarse mediante mecanismos de autenticación multifactor (MFA).

9. Los usuarios únicamente contarán con los accesos y privilegios estrictamente necesarios para el desarrollo de sus funciones, conforme al principio de mínimo privilegio.

10. El incumplimiento de los lineamientos y controles establecidos en la presente política podrá dar lugar a la restricción inmediata de accesos, suspensión de servicios tecnológicos y demás medidas

6.4.2. Gestión de acceso contratistas y seguridad dispositivos personales (BYOD)

1. El acceso a recursos corporativos desde dispositivos personales solo será autorizado a contratistas una vez se haya formalizado y firmado el respectivo contrato con la Corporación Ruta N.
2. Los equipos de colaboradores externos (contratistas) podrán ser sujetos a auditoría con el fin de verificar el cumplimiento de las siguientes condiciones:

- Red WiFi segmentada y habilitada específicamente para contratistas.
- Aplicación obligatoria del modelo de seguridad definido para el acceso a aplicaciones mediante navegador web.
- No se permitirá el uso de VPN de cliente completo para contratistas, salvo autorización expresa y justificada por parte de la Dirección, Subdirección o Secretaría General.

3. El dispositivo personal utilizado dentro de la Corporación deberá cumplir como mínimo con los siguientes requisitos:

   - Sistema operativo con soporte vigente del fabricante.
   - Solución antivirus/EDR activa, vigente y actualizada (incluida la del fabricante, siempre que se encuentre soportada).
   - Firewall habilitado.
   - Bloqueo automático de sesión por inactividad con un máximo de 5 minutos.
   - Se recomienda el cifrado de disco, especialmente cuando se maneje información sensible (no obligatorio).
   - Sesión protegida mediante contraseña con mínimo 8 caracteres y complejidad (mayúsculas, minúsculas, números y caracteres especiales).

4. Queda expresamente prohibido:

   - Almacenar información de la Corporación en el disco local sin autorización del responsable del activo. El almacenamiento deberá realizarse exclusivamente en las plataformas corporativas autorizadas, tales como SharePoint o OneDrive.
   - Desactivar, desinstalar o modificar las herramientas de seguridad instaladas o exigidas por la Corporación, salvo autorización previa y expresa aceptada por escrito por el contratista.
   - Conectarse a la red de Ruta N o acceder a recursos corporativos desde dispositivos que presenten software malicioso, compromisos de seguridad o comportamientos anómalos. En caso de identificarse actividad que represente riesgo para la infraestructura o la información, la Corporación podrá bloquear de manera inmediata el acceso al dispositivo. No se ejercerá control sobre el software instalado por el usuario fuera del entorno corporativo, siempre que este no afecte la seguridad durante la conexión.
   - Conectarse a la red corporativa cuando el dispositivo presente evidencias de compromiso de seguridad.

5. El contratista es responsable de mantener su dispositivo en condiciones seguras durante toda la vigencia de su relación contractual con la Corporación.

6. El acceso a dispositivos, VPN y correo corporativo deberá realizarse mediante autenticación multifactor (MFA).
7. Los usuarios contarán únicamente con los accesos y privilegios estrictamente necesarios para el cumplimiento de sus funciones, bajo el principio de mínimo privilegio.

8. La Corporación se reserva el derecho de bloquear el acceso a recursos corporativos cuando se identifiquen incumplimientos o condiciones de riesgo, sin perjuicio de las demás acciones contractuales o legales a que haya lugar.
9. Contratistas con equipos asignados por la Corporación:

    - En procesos que involucren información de alto valor o cuando la Corporación lo considere necesario, podrán asignarse equipos corporativos a contratistas designados. Estos deberán cumplir los mismos lineamientos, políticas y controles aplicables a los colaboradores vinculados, especialmente en lo relacionado con el uso, custodia y seguridad de los equipos.
    - Se prohíbe el uso de los equipos corporativos para fines personales o actividades ajenas a las funciones contractuales.

6.4.3. Gestión de acceso invitados

1. El acceso a la red de invitados se realizará exclusivamente a través de la red WiFi habilitada para tal fin, la cual se encuentra segmentada y no permite acceso a recursos internos de la Corporación.
2. La conexión requerirá autenticación mediante portal cautivo, con la aceptación previa de los términos y condiciones establecidos para el uso del servicio.
3. El servicio de conectividad podrá estar sujeto a restricciones de ancho de banda, de acuerdo con las necesidades operativas de la Corporación, sin que sea obligatorio notificar previamente dichos límites. En todo caso, se garantizarán parámetros técnicos razonables que permitan la operación normal de los usuarios y el acceso a los servicios y contenidos esenciales de conectividad.
4. La Corporación Ruta N se reserva el derecho de administrar, supervisar y regular el uso de su red. En consecuencia, podrá bloquear o restringir el acceso a contenidos, sitios o servicios que sean considerados nocivos, ilegales, violentos, inapropiados o que representen riesgos de seguridad, afecten la integridad de la comunidad Ruta N o puedan generar perjuicios a terceros. Estas medidas se adoptarán con el fin de garantizar un entorno digital seguro, responsable y alineado con las políticas de uso aceptable de la Corporación.
5. Para invitados directos de la Corporación, el acceso a la red de invitados del piso 2 se realizará exclusivamente mediante los habladores habilitados en las salas de reunión de la Corporación. Esta red se encuentra segmentada y no permite acceso a recursos internos.
6. Queda expresamente prohibido:
    - Conectar dispositivos que realicen escaneo de red, ataques o cualquier actividad maliciosa. Estos equipos serán bloqueados de manera inmediata y podrán ser incluidos en listas de bloqueo permanente.
    - Intentar acceder, de forma directa o indirecta, a recursos internos, servidores, VLAN corporativas o cualquier servicio restringido de Ruta N.
    - Instalar u operar dispositivos o servicios que redistribuyan la conexión de red, tales como hotspots, repetidores, routers personales o túneles no autorizados.
7. La Corporación no se hace responsable por la seguridad, integridad o confidencialidad de los dispositivos personales conectados a la red de invitados.

8. El acceso a la red podrá ser bloqueado de manera inmediata ante la detección de cualquier actividad anómala o potencialmente maliciosa.

6.5. Controles de seguridad tecnológica

La Corporación Ruta N dispone de controles tecnológicos de seguridad diseñados para proteger su infraestructura, redes, dispositivos y activos de información frente a amenazas internas y externas. Estos controles forman parte de la operación habitual de la Corporación, son administrados por el proceso de TI y su cumplimiento es obligatorio para todas las personas que interactúan con la infraestructura tecnológica institucional.

En la operación diaria se mantienen, como base, los siguientes controles:

- Arquitectura de seguridad perimetral y segmentación de red, orientada a limitar el tráfico no autorizado y evitar el movimiento indebido entre redes.
- Implementación de autenticación multifactor (MFA) en todos los accesos corporativos, en la medida en que las aplicaciones o plataformas lo permitan.
- Gestión y remediación de vulnerabilidades técnicas, la cual debe ejecutarse de manera prioritaria e inmediata, respetando como tiempo máximo los definidos para el nivel de criticidad más bajo en los Acuerdos de Nivel de Servicio (ANS) del área de TI.
- Ejecución periódica de pruebas de penetración sobre la infraestructura crítica, con el fin de identificar y mitigar posibles riesgos de seguridad.

Las herramientas y tecnologías que soportan estos controles son definidas, administradas y mantenidas por el proceso de TI, y su uso constituye una condición necesaria para el acceso y la utilización de la infraestructura tecnológica de la Corporación.

6.6. Gestión de Incidentes

1. Todo colaborador o tercero que identifique un evento sospechoso o un incidente de seguridad de la información deberá reportarlo tan pronto como tenga conocimiento de este.
2. El canal oficial para el reporte de incidentes es el correo electrónico ciberseguridad@rutanmedellin.org. En caso de no ser posible utilizar este medio, el incidente deberá ser informado directamente al personal de TI, con el fin de garantizar su registro y gestión oportuna.
3. La gestión de incidentes contempla las fases de identificación, análisis, contención, erradicación, recuperación y documentación de lecciones aprendidas, con el objetivo de minimizar los impactos y prevenir su recurrencia.
4. Cuando un incidente sea clasificado como de alto impacto o tenga relevancia institucional, deberá ser informado a la Dirección Ejecutiva en un plazo máximo de veinticuatro (24) horas o conforme al nivel de criticidad definido.
5. Todos los incidentes deberán ser debidamente documentados, gestionados hasta su cierre y, cuando aplique, deberán incluir el registro de acciones de mejora orientadas a la prevención de futuros eventos.

6.7. Concientización y cultura

Se desarrollarán programas permanentes orientados a fortalecer la cultura de seguridad de la información en la Corporación, los cuales incluyen:

1. Sensibilización en ciberseguridad: programas orientados a que los colaboradores reconozcan los riesgos digitales y comprendan la importancia de proteger adecuadamente la información institucional.

2. Capacitación por niveles organizacionales: procesos de formación adaptados al rol y nivel de responsabilidad de cada área, con el fin de asegurar que todos los colaboradores cuenten con las competencias necesarias para identificar y responder adecuadamente ante posibles amenazas.

3. Promoción de buenas prácticas: iniciativas enfocadas en fomentar hábitos seguros en el uso de la tecnología, tales como el uso de contraseñas robustas, la actualización periódica de equipos y la prevención de accesos no autorizados a la información o a los sistemas corporativos.

6.8. Cumplimiento

La seguridad de la información no depende únicamente de herramientas tecnológicas; también requiere del compromiso y la atención diaria de las personas que hacen parte de la Corporación. Por ello, se mantendrán acciones permanentes de sensibilización y formación que permitan reconocer riesgos, usar adecuadamente las plataformas y proteger la información institucional en el trabajo cotidiano.

De manera continua se realizarán actividades de:

- Sensibilización en ciberseguridad.
- Capacitación según el rol y nivel de responsabilidad.
- Promoción de buenas prácticas en el uso de equipos, redes y sistemas.
- Comunicaciones internas y ejercicios prácticos que refuercen la prevención de incidentes.

Cada colaborador deberá participar en las actividades relacionadas con seguridad de la información. Esta participación hace parte de las responsabilidades propias del rol y su incumplimiento podrá ser considerado dentro de los procesos internos de seguimiento.

Estas acciones se integran a la gestión general de la seguridad de la información de la Corporación Ruta N, la cual se desarrolla de forma progresiva mediante políticas, controles y procedimientos que se publican y actualizan cuando es necesario. La gestión se enfoca en prevenir incidentes, detectar oportunamente situaciones de riesgo, responder cuando ocurran eventos y fortalecer los controles a partir de la experiencia y las lecciones aprendidas.

6.9. Revisión y actualización

Esta política será revisada al menos una vez al año, o de manera anticipada cuando se presenten cambios significativos en el entorno tecnológico, normativo o en el panorama de amenazas que puedan afectar su vigencia o aplicabilidad.

Certificado de firma

Para los efectos legales pertinentes, **las partes manifiestan que han decidido suscribir el presente documento de manera electrónica** , y declaran que la firma estampada en el mismo ha sido puesta por quien dice ser su firmante cumpliendo todos los requisitos legales para este tipo de firmas, y por ello,**reconocen la plena validez tanto de lo dispuesto en el clausulado del presente documento** como de las firmas electrónicas que en él se asientan.

Autenticidad

VYD

Virmar Yessid David
Autenticado con:
Correo electrónico
Código OTP

Hash de firmante:
7666d1b160d7f350562aaf9436fd7c9b2f5352af11dd4290c101c32d5556dec8

E-mail	yessid.david@rutanmedellin.org
IP	177.253.222.170
Rol	Firmante
Firmado	22/5/26, 15:57:29 GMT-5

JA

Javier Arcila
Autenticado con:
Correo electrónico
Código OTP

Hash de firmante:
b3637f3d9edcf5ce24558188814e769395dfc45ff0f4508e7cc2499c06e67873

E-mail	javier.arcila@rutanmedellin.org
IP	177.253.222.250 Medellín, Antioquia, Colombia
Rol	Firmante
Firmado	25/5/26, 10:26:56 GMT-5

JO

Jaiber Ortiz
Autenticado con:
Correo electrónico
Código OTP

Hash de firmante:
b7b2d6625e623bd795cfbb14770654df7929fd8314c8b34ffa7b631c5d7f158c

E-mail	jaiber.ortiz@rutanmedellin.org
IP	177.253.222.250 Medellín, Antioquia, Colombia
Rol	Firmante
Firmado	25/5/26, 14:22:27 GMT-5

SM

Sebastián Marín
Autenticado con:
Correo electrónico
Código OTP

Hash de firmante:
59476c634400a6b4e38113e90cbbfc7005898276a626d838feb33d9a0761f944

E-mail	sebastian.marin@rutanmedellin.org
IP	177.253.222.250
Rol	Firmante
Firmado	25/5/26, 14:29:04 GMT-5

AC

Alexander Cuspoca
Autenticado con:
Correo electrónico
Código OTP

Hash de firmante:
0642ac44669854da4665f85795714b5ebe7a60abde961dd97e34f52499a586c1

E-mail	alexander.cuspoca@rutanmedellin.org
IP	177.253.222.170 Minato-ku, Japan
Rol	Firmante
Firmado	25/5/26, 14:30:21 GMT-5

CL

Carolina Londoño
Autenticado con:
Correo electrónico
Código OTP

Hash de firmante:
910d6d23bd2ebd7ae620bbde89735a27d514787450227631855fd99f37ff98f8

E-mail	direccionejecutiva@rutanmedellin.org
IP	181.71.129.31 Envigado, Antioquia, Colombia
Rol	Firmante
Firmado	25/5/26, 15:41:37 GMT-5

Integridad del documento

Número de documento: K9XYOX5CZD

Función Hash: SHA-256

Hash del documento: 2864bbc1b0ff885ae009be09c374c472a3d41a42d86d32491d98fc31074b268b

Disponibilidad del documento

El documento puede ser consultado a través de su número de identificación y/o código QR en nuestra plataforma **www.auco.ai/verify**