**CORPORACIÓN DE LA INDUSTRIA AERONÁUTICA COLOMBIANA. CIAC S.A.**

# MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código: M-7-00-005
Versión: 6
Fecha de Actualización: 8 de octubre de 2025

AV. Calle 26 No. 103-08 Entrada 1, Interior 2
Bogotá D.C – Colombia

# CONTROL DE EMISIÓN

| ELABORÓ | REVISÓ | APROBÓ |
|---|---|---|
| Nombre:<br>TE. JESSICA TATIANA CIFUENTES DIMAS | Nombre:<br>LUISA CAROLINA SABAS ECHAVARRIA<br>Cargo:<br>Vicepresidenta Administrativa<br>Nombre:<br>ALEJANDRA BERNAL WESSO<br>Cargo:<br>Grupo SICA<br>Nombre:<br>RAFAEL ALBERTO VELASQUEZ GARAVITO | Nombre:<br>MG. ANDRÉS GUZMÁN MORALES |
| Cargo:<br>Coordinadora Grupo TICS | Cargo:<br>Representante Alta Dirección | Cargo:<br>Presidente |

# CONTROL DE CAMBIOS

| VERSIÓN | DESCRIPCIÓN DEL CAMBIO | ELABORÓ | FECHA |
|---|---|---|---|
| 6 | Se actualizó el documento conforme a la nueva plantilla definida por el SIGCA. Se reorganizó el contenido tomando como referencia la estructura del Manual de Políticas del Sistema de Gestión de Seguridad de la Información del MinTIC y se incorporó la política general de seguridad y privacidad de la información, lo cual permitió eliminar el documento POL-1-01-009 “Políticas de Seguridad de la Información”. Se retiró la palabra “política” en los diferentes apartados, conforme a las directrices del SIGCA. Se realizaron mejoras en la redacción general, eliminando repeticiones y ajustando los lineamientos para mayor claridad. Las listas con viñetas fueron reemplazadas por listas ordenadas alfabéticamente, facilitando su referencia. Se integraron los lineamientos sobre el uso de los recursos tecnológicos en un único numeral y se incluyó la seguridad de dispositivos móviles dentro del apartado de seguridad física y del entorno. Asimismo, se incorporaron los apartados de criptografía, relación con proveedores, gestión de la continuidad del negocio, y sensibilización y comunicación. Se eliminó el numeral específico de OneDrive, el cual fue integrado en el apartado de almacenamiento en la nube, dentro de medios de almacenamiento. También se suprimió el numeral sobre acuerdos de niveles de servicio, ya que dicho tema se encuentra abordado en el procedimiento de soporte técnico a servicios informáticos. | TE. JESSICA TATIANA CIFUENTES DIMAS | 8 de octubre de 2025 |
| | | | |
| | | | |

# TABLA DE CONTENIDO

# 1 INTRODUCCIÓN

En un entorno digital cada vez más interconectado y expuesto, las amenazas que comprometen la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información se han intensificado, generando riesgos significativos tanto para las organizaciones como para las personas. En este contexto, el Manual de Seguridad y Privacidad de la Información se elabora con el propósito de establecer políticas, lineamientos y buenas prácticas que aseguren un manejo adecuado de la información digital, previniendo accesos no autorizados, alteraciones, pérdidas o filtraciones que puedan comprometer la privacidad de los usuarios y la reputación de la Corporación de la Industria Aeronáutica Colombiana – CIAC.

Este manual proporciona directrices claras para la implementación con el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno Digital y para el cumplimiento de los requisitos legales y reglamentarios aplicables en materia de protección de la información. Igualmente, busca fortalecer la cultura organizacional en materia de seguridad digital y ciberseguridad, brindando a funcionarios, contratistas, pasantes, aprendices, proveedores y demás terceros las herramientas necesarias para identificar, prevenir y responder eficazmente a las amenazas del entorno digital.

## 1.1 OBJETIVO

Establecer políticas, lineamientos y buenas prácticas que garanticen la protección de la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información, así como de la infraestructura tecnológica, mediante la implementación de medidas de seguridad tanto técnicas como organizativas. Estas medidas buscan fortalecer una cultura organizacional orientada a la ciberseguridad y asegurar el cumplimiento de la legislación vigente, con el fin de prevenir accesos no autorizados, alteraciones, pérdidas o filtraciones de datos e información que puedan comprometer la privacidad de los usuarios y afectar la reputación de la Corporación de la Industria Aeronáutica Colombiana – CIAC

## 1.2 ALCANCE

Este manual aplica a todo el personal de la Corporación, incluyendo funcionarios, contratistas, pasantes, aprendices, proveedores y demás partes interesadas que tengan acceso a la información y/o a la infraestructura tecnológica de la Corporación de la Industria Aeronáutica Colombiana – CIAC.

El alcance del manual comprende los siguientes aspectos:

- **Información sensible y crítica:** Toda información en formato digital gestionada por la Corporación que se considere sensible o crítica para la operación, privacidad y seguridad de la organización. Esto incluye datos personales, técnicos, financieros, operativos y estratégicos.

- **Infraestructura tecnológica:** Equipos informáticos, sistemas de información, redes, dispositivos y demás recursos tecnológicos utilizados para almacenar, procesar, transmitir o acceder a la información digital de la Corporación.

## 1.3 DOCUMENTOS DE REFERENCIA

### 1.3.1 Estructura Documental SIGCA:

- Manual del Sistema Integrado de Gestión de la Calidad Aeronáutica.

### 1.3.2 Otros Documentos De Referencia:

- Política de Gobierno Digital
- Modelo de Seguridad y Privacidad de la Información – MSPI del MinTIC
- Modelo Integrado de Planeación y Control - MIPG
- Norma ISO IEC 27001
- 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”
- Resolución No. 013 de 2023 - "Por medio de la cual se adopta la política para el tratamiento de datos personales, se designa y establecen las competencias del oficial de datos personales de la Corporación de la Industria Aeronáutica Colombiana S.A."
- Resolución 7870 de 2022 – “Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.”
- Resolución 1519 de 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 materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.”

## 1.4 TÉRMINOS & DEFINICIONES

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de Información y Recursos:** Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016)
- **Administración De Usuarios:** Conjunto de actividades relacionadas con la creación, modificación, asignación de roles y control de accesos a los sistemas, de acuerdo con los perfiles definidos.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **ANS:** Acuerdos de Nivel de Servicio
- **Autenticidad:** Seguridad de que un mensaje, una transacción u otro intercambio de información proviene de la fuente de la que afirma ser. Autenticidad implica prueba de identidad. (ISO/IEC 27000).
- **Buena Práctica:** Método recomendado que se considera óptimo, debido a los resultados positivos que ha generado en situaciones previas.
- **Ciberdelincuente:** Persona que busca sacar beneficio de los problemas o fallos de seguridad encontrados en programas, servicios, plataformas o herramientas, utilizando distintas técnicas como la ingeniería social o el malware (https://www.incibe.es/aprendeciberseguridad/)
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados. (Resolución 7870 de 2022)
- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a personas, entidades o procesos autorizados. (ISO/IEC 27000)
- **Copia de Seguridad (Backup):** Duplicado de los datos que se hace para poder recuperarlos ante cualquier pérdida o incidente. (www.ticportal.es/glosario-tic)
- **Custodio:** Es la unidad organizacional o proceso, designado por la Corporación para mantener las medidas de protección necesarias sobre los activos de información confiados.
- **Directriz:** Instrucción o norma que ha de seguirse en la ejecución de algo (RAE)
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera (ISO/IEC 27000)
- **Dispositivo Móvil:** Dispositivo destinado a almacenar y reproducir archivos digitales como audio, imágenes y vídeo, con la capacidad de conectarse a internet, permitiendo enviar y compartir los archivos capturados. Los dispositivos móviles más utilizados son los computadores portátiles, tabletas, cámaras, teléfonos inteligentes o smartphones, reproductores inteligentes, entre otros.
- **Firewall:** Aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno (Glosario (mintic.gov.co))
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos (ISO/IEC 27000)
- **Lineamiento:** Instrucciones más específicas que complementan una política y detallan cómo deben implementarse o ejecutarse las directrices establecidas.
- **Malware:** Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas. (Glosario MinTic)
- **Mesa de Ayuda:** Herramienta destinada como único contacto entre los usuarios y Grupo TICS para la atención de requerimientos.

- **MFA:** Autenticación Multifactor
- **Mínimo Privilegio:** Los usuarios, sistemas o aplicaciones deben tener solo los privilegios necesarios para realizar sus tareas o para el desempeño de su trabajo.
- **Necesidad de Saber:** Otorgar acceso a la información solo a aquellas personas que lo necesitan para desempeñar sus funciones específicas dentro de la Corporación.
- **No Repudio:** Servicio que tiene como objetivo evitar que una persona o una entidad niegue que ha realizado una acción de tratamiento de datos, proporcionando la prueba de distintas acciones de red, garantizando la disponibilidad de pruebas que pueden presentarse a terceros y utilizarse para demostrar que un determinado evento o acción si ha tenido lugar. (https://colombiatic.mintic.gov.co )
- **OJT:** On the Job Training SAP, Entrenamiento para desempeño según funciones de usuario.
- **OneDrive:** Herramienta de almacenamiento en la nube y uso compartido de archivos
- **Página Web**: Conjunto de informaciones de un sitio web que se muestran en una pantalla y que puede incluir textos, contenidos audiovisuales y enlaces con otras páginas.
- **Perfil De Acceso:** Conjunto de autorizaciones asignadas a un usuario que determinan las funciones, transacciones o información a las que puede acceder dentro de un sistema. Los perfiles se configuran en función del rol y responsabilidades del usuario.
- **Personal en Comisión:** Colaboradores que asisten como representantes de la CIAC a comités, reuniones, conferencias, seminarios, talleres, ferias u otros eventos relacionados con sus funciones u obligaciones dentro o fuera del país.
- **Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico. (Guía No. 2 Seguridad y Privacidad de la Información MinTic)
- **Propietario de la Información:** Es una parte designada de la Corporación, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. (Guía No. 5 Seguridad y Privacidad de la Información MinTic)
- **Recursos Tecnológicos:** Componentes de hardware y software tales como servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros; los cuales tienen como finalidad apoyar las tareas administrativas y logísticas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Corporación.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000)
- **Seguridad Digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales. (Modelo de Seguridad y Privacidad de la Información - MinTIC)
- **Sistema de información.** Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información requiriendo a su vez de la interacción de uno o más activos de información para efectuar las tareas previstas. Puede ser de origen interno o de origen externo conforme a las necesidades de la Corporación.

- **Sitio Web:** Conjunto de páginas web agrupadas bajo un mismo dominio de internet (RAE)
- **Ticket:** Número de proceso o caso registrado en la herramienta destinada como mesa de ayuda para la atención de requerimientos de Grupo TICS
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

# 2 DESARROLLO

## 2.1 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Corporación de la Industria Aeronáutica Colombiana - CIAC, consciente de la importancia de proteger su información en un entorno digital dinámico y expuesto a múltiples riesgos, se compromete con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), orientado a preservar la confidencialidad, integridad, disponibilidad, privacidad, autenticidad, confiabilidad y no repudio de la información, así como a proteger los activos tecnológicos asociados.

Este compromiso se traduce en la adopción de políticas, procedimientos, controles técnicos y organizativos, y en la gestión efectiva de riesgos e incidentes, fomentando una cultura organizacional en materia de seguridad de la información, seguridad digital y ciberseguridad entre funcionarios, contratistas, pasantes, aprendices, proveedores y demás partes interesadas, con el fin de contribuir al mejoramiento continuo y al cumplimiento de los objetivos misionales y corporativos.

### 2.1.1 Objetivos

a. Fortalecer la confidencialidad, integridad, disponibilidad, confiabilidad, privacidad, autenticidad y no repudio de la información gestionada por la Corporación.
b. Establecer lineamientos para la gestión de riesgos, la atención de incidentes y la implementación de controles relacionados con la seguridad y privacidad de la información, la seguridad digital y la ciberseguridad, conforme a la normativa vigente.
c. Definir las directrices para el manejo adecuado de la información digital y de los recursos tecnológicos institucionales.
d. Promover y consolidar una cultura organizacional orientada a la seguridad de la información, la seguridad digital y la ciberseguridad, que contribuya a minimizar la materialización de riesgos asociados a incidentes cibernéticos que puedan afectar los activos de información de la Corporación.

## 2.2 ROLES Y RESPONSABILIDADES

**Alta Dirección**

a. Impulsar y respaldar los proyectos relacionados con la seguridad de la información, la seguridad digital y la ciberseguridad.
b. Articular los esfuerzos, recursos y estrategias institucionales para garantizar la implementación, sostenibilidad y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI).
c. Velar por la adopción, cumplimiento y actualización de las políticas, lineamientos y directrices en materia de seguridad de la información, seguridad digital y ciberseguridad.
d. Promover una cultura organizacional orientada a la protección de la información y al fortalecimiento de la seguridad digital y la ciberseguridad en todos los niveles de la Corporación.

**Comité Institucional de Gestión y Desempeño**

a. Asegurar la implementación, seguimiento y mejora de las políticas, lineamientos y directrices en materia de seguridad de la información, seguridad digital y ciberseguridad.
b. Realizar el seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la adecuada implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).
c. Aprobar acciones, iniciativas y mejoras que contribuyan al fortalecimiento de la seguridad digital, la privacidad de la información y la gestión de riesgos asociados.
d. Emitir recomendaciones y conceptos que apoyen el análisis y la toma de decisiones corporativas en materia de seguridad de la información, seguridad digital y ciberseguridad.

**Oficina de Control Interno**

a. Realizar el seguimiento al cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), así como de las políticas, lineamientos y controles relacionados con la seguridad de la información, seguridad digital y ciberseguridad.
b. Emitir observaciones, recomendaciones y planes de mejora en el marco del ejercicio del control interno, con el fin de fortalecer la gestión de riesgos y el cumplimiento de los principios de seguridad y privacidad de la información.

**Grupo TICS**

a. Desarrollar e implementar políticas, controles y mecanismos técnicos que garanticen la confidencialidad, integridad, disponibilidad, privacidad, autenticidad y no repudio de la información y de los activos digitales de la Corporación.

b. Alinear la estrategia de seguridad de la información, seguridad digital y ciberseguridad con los objetivos corporativos.
c. Coordinar y ejecutar las actividades relacionadas con la gestión de incidentes de seguridad de la información, seguridad digital y ciberseguridad.
d. Identificar, analizar, documentar y reportar los incidentes que afecten la seguridad de los activos de información.
e. Revisar periódicamente los controles establecidos y proponer ajustes para mitigar los riesgos identificados.
f. Acompañar a los líderes de proceso en la identificación y tratamiento de riesgos relacionados con la seguridad de la información, seguridad digital y ciberseguridad, de acuerdo con las metodologías y disposiciones establecidas
g. Administrar y custodiar los sistemas de información bajo su responsabilidad, garantizando su funcionamiento seguro y continuo.
h. Diseñar y ejecutar campañas de sensibilización y formación dirigidas al personal, en temas de seguridad de la información, seguridad digital y ciberseguridad, en coordinación con el CECSA cuando aplique.

**Oficina Jurídica**

a. Identificar y analizar los aspectos legales y normativos aplicables en materia de seguridad de la información, seguridad digital y ciberseguridad.
b. Brindar asesoría jurídica a los procesos frente a acciones, medidas o requerimientos relacionados con la seguridad y privacidad de la información, incluyendo eventuales actuaciones ante autoridades competentes.

**Grupo De Talento Humano**

a. Promover la concienciación del personal sobre sus responsabilidades en materia de seguridad de la información, seguridad digital y ciberseguridad, a través de procesos de inducción y reinducción.
b. Gestionar el proceso de vinculación y desvinculación del personal, asegurando la aplicación de los controles establecidos y el cumplimiento de la normativa vigente relacionada con la seguridad y privacidad de la información.

**Vicepresidentes, Jefes, Gerentes o Coordinadores**

a. Identificar los activos de información bajo su responsabilidad y mantener actualizado su inventario, así como los riesgos asociados a la seguridad de la información, seguridad digital y ciberseguridad.
b. Aplicar los controles establecidos para preservar la confidencialidad, integridad, disponibilidad, privacidad, autenticidad y no repudio de la información gestionada en su proceso o área.

c. Establecer los criterios y niveles de acceso a la información y a los sistemas que la soportan, en su calidad de propietario de la información digital, de acuerdo con los lineamientos corporativos.

**Usuarios**

a. Cumplir con las políticas, lineamientos y controles establecidos para garantizar la integridad, disponibilidad, confidencialidad, privacidad, autenticidad y no repudio de la información.
b. Reportar de manera oportuna cualquier incidente o anomalía relacionada con la seguridad de la información, seguridad digital y ciberseguridad.
c. Mantener la confidencialidad de la información que reciba, genere o procese durante el ejercicio de sus funciones en la Corporación.

## 2.3 SEGURIDAD DE LOS RECURSOS HUMANOS

En cumplimiento de la Política General de Seguridad y Privacidad de la Información y con el fin de minimizar los riesgos que puedan afectar la seguridad de la información, la seguridad digital y la ciberseguridad, se establecen los siguientes lineamientos, aplicables a todo el personal que tenga acceso a información o recursos tecnológicos corporativos, incluyendo funcionarios, contratistas, pasantes, aprendices y demás terceros:

a. Realizar la verificación de antecedentes disciplinarios durante el proceso de selección de personal, sin excepción del cargo al que se postulen los candidatos.

b. Exigir la firma de un acuerdo de confidencialidad y manejo responsable de la información a todo el personal que labore en la Corporación.

c. Incluir en los programas de inducción y reinducción contenidos relacionados con seguridad de la información, seguridad digital y ciberseguridad, asegurando que el personal conozca sus responsabilidades y las implicaciones del uso indebido de los activos de información y recursos tecnológicos.

d. Garantizar que los accesos a la información y a los sistemas se otorguen únicamente con base en el rol, las responsabilidades y la necesidad de uso, aplicando los principios de mínimo privilegio necesario y necesidad de saber.

e. Realizar seguimiento al cumplimiento de las políticas y controles de seguridad de la información, seguridad digital y ciberseguridad por parte del personal vinculado.

f. Reforzar el conocimiento del personal mediante campañas de sensibilización periódicas en temas de seguridad de la información, ciberseguridad y uso responsable de los recursos tecnológicos.

g. Asegurar la devolución de los recursos tecnológicos, credenciales e información bajo custodia al momento del retiro o finalización del vínculo con la Corporación.

## 2.4 CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

En concordancia con la Política de Seguridad y Privacidad de la Información se establece los siguientes lineamientos generales para el manejo de la información digital:

a. Toda información digital generada, almacenada o transformada por funcionarios, contratistas, proveedores o terceros utilizando los recursos tecnológicos de la Corporación, o en cumplimiento de sus funciones o contratos, constituye un activo de información propiedad exclusiva de la Corporación de la Industria Aeronáutica Colombiana – CIAC.

b. El acceso a la información digital debe otorgarse conforme a los principios de “necesidad de saber” y “mínimo privilegio”, limitando el acceso únicamente a las personas que requieran dicha información para el desempeño de sus funciones.

c. Todos los usuarios deben asumir la responsabilidad sobre la información digital a la que acceden y que procesan, asegurando su uso adecuado y contribuyendo a salvaguardar la confidencialidad, integridad y disponibilidad de esta.

d. Los jefes, coordinadores o responsables de área deben asegurar la entrega y custodia de la información que administra un colaborador antes de firmar el paz y salvo por traslado, terminación de funciones o desvinculación de la Corporación.

## 2.5 CONTROL DE ACCESOS

En cumplimiento de la Política General de Seguridad y Privacidad de la Información, la Corporación garantiza y limita el acceso a las redes de datos, recursos tecnológicos y sistemas de información mediante la asignación de privilegios de acceso adecuados, asegurando que los usuarios accedan únicamente a la información autorizada, conforme a sus funciones, responsabilidades y niveles de autorización.

El control de accesos se basa en los principios de mínimo privilegio, necesidad de saber y autenticación segura, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información digital corporativa.

### 2.5.1 Gestión De Accesos A Usuarios

El Grupo TICS es responsable de proporcionar y gestionar el acceso a los recursos tecnológicos de la Corporación, tales como el Directorio Activo, equipos de cómputo, correo electrónico corporativo, servicios de Microsoft 365, DataDoc y el ERP SAP. Para esto, se establecen los siguientes lineamientos:

a. Toda solicitud de creación, modificación o suspensión de cuentas debe realizarse a través de la herramienta destinada como mesa de servicios o mediante el correo electrónico soporte.gtics@ciac.gov.co habilitado para tal fin.

b. El acceso a los recursos tecnológicos debe ser solicitado formalmente por el jefe inmediato o un funcionario del área, siempre que cuente con la aprobación de este, y conforme al rol, funciones y nivel de autorización del usuario.

c. Las solicitudes de acceso para usuarios nuevos al ERP SAP deben ser tramitadas exclusivamente por el líder funcional del módulo correspondiente.

d. Los accesos de los usuarios se suspenden durante los periodos de vacaciones, licencias, incapacidades o cualquier otra novedad que requiera su desactivación temporal, con el fin de preservar la seguridad de la información y los recursos tecnológicos de la Corporación.

e. Toda cuenta de usuario es personal e intransferible y está sujeta a los principios de mínimo privilegio y necesidad de saber. Se exceptúan los casos de aprendices, pasantes y personal no esencial, quienes podrán contar con accesos compartidos o genéricos, debidamente justificados y controlados.

f. Cualquier cuenta de acceso a los recursos tecnológicos que no sea utilizada durante un periodo prolongado debe ser desactivada, a fin de reducir los riesgos asociados a accesos no autorizados o innecesarios

g. Al finalizar la relación laboral o contractual, el Grupo TICS revoca de forma inmediata todos los accesos asignados al usuario.

#### 2.5.1.1 Accesos A Recursos Tecnológicos Generales

Con el objetivo de garantizar un acceso controlado y seguro a los recursos tecnológicos corporativos, tales como el Directorio Activo, equipo de cómputo, mesa de servicios, correo electrónico corporativo y la suite de Microsoft 365, se establecen los siguientes lineamientos:

a. La solicitud de nuevos accesos debe contener los siguientes datos:

- Nombres y apellidos completos
- Número de documento de identificación
- Nombre del cargo
- Teléfono de contacto
- Fecha de vinculación
- Fecha de la inducción general corporativa
- Número de activo fijo del equipo de cómputo asignado.

b. La creación de accesos está condicionada a la participación del usuario en una inducción sobre ciberseguridad. En caso de que la inducción general corporativa esté programada para una fecha posterior al inicio de la vinculación laboral, se coordina con el Grupo TICS una inducción personalizada en ciberseguridad con el fin de no afectar las actividades laborales. El Grupo de Talento Humano valida la asistencia del usuario a la sesión correspondiente. En caso de no asistir, no se gestiona el acceso a los recursos tecnológicos.

c. Se verifica con el Grupo Administrativa la asignación del equipo de cómputo antes de habilitar el acceso.

d. La cuenta del usuario se bloquea tras cinco (5) intentos fallidos consecutivos de inicio de sesión. Para desbloquearla, el usuario debe solicitar formalmente el restablecimiento a través de los canales establecidos.

e. Al finalizar la relación laboral o contractual, el propio usuario o un funcionario autorizado del grupo debe gestionar la cancelación de los accesos. Esta solicitud debe tramitarse incluso si el usuario no cuenta con accesos activos, ya que el número de solicitud se requiere para ser incluido en el formato de paz y salvo correspondiente.

#### 2.5.1.2 Accesos Para Personal En Comisión

Con el fin de garantizar el acceso continuo y seguro a los recursos tecnológicos por parte del personal que se encuentre en comisión para asistir a conferencias, seminarios, talleres, ferias u otros eventos relacionados con sus funciones u obligaciones, tanto a nivel nacional como internacional, se establecen los siguientes lineamientos:

a. Informar oportunamente al Grupo TICS sobre el personal en comisión, proporcionando la siguiente información para asegurar la continuidad del acceso a los recursos tecnológicos necesarios durante el periodo establecido:

    - Nombres y apellidos completos del usuario.
    - Fecha de inicio y finalización de la comisión.

- Ubicación física donde se desarrollará la comisión (Incluir ciudad, departamento y/o país).
- Lista detallada de los recursos tecnológicos requeridos (por ejemplo: acceso a sistemas internos, correo corporativo, software específico, dispositivos, entre otros).
- Indicar si se requiere acceso a información confidencial o sensible, y si se requiere el uso de VPN.
- Número de contacto para atención de posibles incidentes técnicos durante la comisión y el Grupo TICS pueda comunicarse directamente.

b. La solicitud debe realizarse con al menos dos (2) días de antelación a la salida en comisión, con el fin de que el Grupo TICS pueda evaluar los requerimientos y gestionar los accesos necesarios.

c. En caso de requerirse desbloqueos o configuraciones especiales, la solicitud debe contar con la aprobación de la Coordinación del Grupo TICS.

d. Es obligatorio seguir las medidas de seguridad establecidas, incluyendo el uso de VPN cuando se acceda a información corporativa desde ubicaciones externas, para garantizar la protección de los recursos tecnológicos.

e. Una vez revisada la solicitud, el Grupo TICS informa si los recursos están disponibles durante la comisión y confirma que los accesos no son bloqueados por los mecanismos de seguridad.

f. En caso de no realizar la solicitud correspondiente, los accesos del usuario se bloquean automáticamente y se catalogan como intentos de intrusión cibernética.

#### 2.5.1.3 Accesos ERP SAP

Con el fin de asegurar un control adecuado sobre los accesos, roles y privilegios de los usuarios en el ERP SAP, se establecen los siguientes lineamientos:

a. Para la creación de nuevos usuarios, la solicitud debe incluir el Formato OJT debidamente diligenciado y firmado por el líder funcional del módulo correspondiente. Además, se debe proporcionar los siguientes datos:

   - Transacciones requeridas según el cargo a desempeñar
   - Nombres y apellidos completos
   - Número de documento de identificación
   - Teléfono de contacto
   - Correo electrónico
   - Nombre del cargo y dependencia.

b. Las solicitudes para asignación de transacciones, activación de licencias, modificación o cancelación de accesos al SAP pueden ser gestionadas por cualquier funcionario autorizado, siempre que cuenten con la aprobación del líder funcional del módulo correspondiente.

c. Las cuentas de usuario se crean de forma individual, con el fin de establecer responsabilidades en la administración de accesos, y conforme a la disponibilidad de licencias existentes.

d. La cuenta del usuario se bloquea automáticamente tras tres (3) intentos fallidos de inicio de sesión consecutivos. Para su desbloqueo, el usuario debe realizar la solicitud formal a través de los canales establecidos.

e. Mensualmente, o cuando se considere necesario, el Profesional Controller de Operaciones y Proyectos SAP/SuccessFactors realiza una verificación con los líderes funcionales de los módulos SAP, con el fin de validar que los roles y perfiles asignados se ajusten a las funciones reales de los usuarios. Asimismo, se garantiza la inactivación de los accesos del personal retirado y la correspondiente actualización de la matriz de roles y perfiles.

#### 2.5.1.4 Accesos SuccessFactors

Con el fin de garantizar un control adecuado sobre los accesos, roles y privilegios de los usuarios en SuccessFactors, se establecen los siguientes lineamientos:

a. La creación de usuarios para el personal de planta y militar es gestionada exclusivamente por el Grupo de Talento Humano.

b. La cuenta del usuario se bloquea automáticamente tras cinco (5) intentos fallidos de inicio de sesión consecutivos. En caso de bloqueo o de olvido de la contraseña, el usuario debe realizar la solicitud formal de desbloqueo o restablecimiento a través de los canales establecidos.

c. Al finalizar la relación laboral, el Grupo de Talento Humano es responsable de la inactivación de los usuarios en SuccessFactors, por lo cual no se requiere generar solicitudes adicionales para este proceso.

#### 2.5.1.5 Accesos DataDoc

Con el fin de asegurar un control adecuado sobre los accesos de los usuarios a DataDoc, se establecen los siguientes lineamientos:

a. La creación de usuarios debe cumplir con los lineamientos definidos en el numeral Acceso A Recursos Tecnológicos Generales.

b. El usuario debe estar registrado en el Directorio Activo y contar con los siguientes datos diligenciados:

- Nombres y apellidos completos
- Correo electrónico
- Número de documento de identificación
- Nombre del cargo
- Grupo o área al que pertenece el usuario
- Número de contacto.

c. Para el personal que tiene asignado correo electrónico, el nombre de usuario será el mismo que su correo, es decir: i.apellido@ciac.gov.co. Para el personal que no dispone de correo electrónico, se utilizará el mismo formato (i.apellido@ciac.gov.co) con el nombre de usuario creado en el Directorio Activo.

d. La contraseña de DataDoc se sincroniza con la contraseña del equipo de cómputo, por lo que se actualizará automáticamente cuando esta sea modificada.

e. Los roles y perfiles de acceso serán asignados por la Oficina de Planeación, de acuerdo con las funciones u obligaciones contractuales del personal.

### 2.5.2 Derechos De Acceso Privilegiado

El Grupo TICS restringe y controla la asignación y uso de los derechos de acceso privilegiado a los recursos tecnológicos de la Corporación, asegurando que estos se administren bajo condiciones controladas y seguras. Estos privilegios, por su nivel de sensibilidad, requieren medidas específicas de supervisión y control, por lo que se establecen los siguientes lineamientos:

a. Otorgar privilegios de administración únicamente al personal expresamente designado para estas funciones, como es el caso del Grupo TICS (Coordinador, Profesional de Infraestructura y Técnicos de Operaciones) para los recursos tecnológicos generales. En el caso del sistema ERP SAP, el personal autorizado con perfil de administrador corresponde exclusivamente al Coordinador del Grupo TICS y a la Profesional Controller De Operaciones Y Proyectos Sap/SuccessFactors.

b. Establecer cuentas personalizadas con privilegios elevados para cada usuario administrador, a fin de asegurar la trazabilidad de sus actividades.

c. En caso de requerir una cuenta con perfil de administrador, se deberá realizar una solicitud formal a la Vicepresidencia Administrativa, justificando la necesidad. Esta deberá contar con el visto bueno de la Coordinación del Grupo TICS y estará sujeta a evaluación y aprobación.

d. Restringir las conexiones remotas a los recursos tecnológicos, permitiendo únicamente el acceso a personal autorizado.

e. Eliminar, renombrar o inhabilitar las cuentas y contraseñas predeterminadas que vienen por defecto en los recursos tecnológicos.

f. Configurar los equipos de cómputo con restricciones que impidan la instalación de programas o herramientas que otorguen acceso privilegiado sin autorización, y verificar que los usuarios finales no cuenten con software o utilitarios que puedan vulnerar los controles de seguridad establecidos.

g. Prohibir el uso de software o herramientas que permitan evadir los controles de seguridad definidos para los recursos tecnológicos.

h. Revocar inmediatamente los accesos privilegiados cuando el personal deje de cumplir con las funciones que justifican estos accesos o cuando se detecten incidentes de seguridad relacionados con su uso.

### 2.5.3 Acceso A Sistemas Y Aplicaciones

Con el objetivo de garantizar la seguridad de los sistemas de información y aplicaciones utilizadas en la Corporación, se implementan controles de acceso adecuados y se establecen los siguientes lineamientos:

a. El jefe, gerente o coordinador de oficina o grupo, como propietario de los sistemas o aplicaciones que respaldan los procesos a su cargo, es responsable de la asignación, modificación y revocación de los privilegios de acceso correspondientes.

b. Los accesos son revisados periódicamente por los responsables de cada sistema o aplicación para asegurar que continúan siendo apropiados. Cualquier acceso innecesario o no autorizado se revoca de manera inmediata.

c. El jefe, gerente o coordinador es responsable de la administración de los sistemas de información o aplicaciones externas bajo su cargo, y debe velar por la confidencialidad e integridad de la información que gestionan.

d. El Grupo TICS mantiene un consolidado general de las plataformas externas utilizadas por la Corporación; sin embargo, cada grupo es responsable de mantener actualizado el inventario de sistemas o aplicaciones bajo su administración y de garantizar el cumplimiento de los lineamientos de seguridad.

### 2.5.4 Acceso A Redes Y Servicios De Red

El Grupo TICS, como responsable de la administración y seguridad de las redes de datos y servicios de red de la Corporación, adopta mecanismos de control de acceso lógico, así como medidas preventivas, correctivas y de monitoreo para proteger estos recursos contra accesos no autorizados, por lo que se establecen los siguientes lineamientos:

a. Los equipos de cómputo que se conecten a las redes de datos deben estar integrados en el dominio de la Corporación, contar con protección antivirus y tener instaladas las últimas actualizaciones y parches de seguridad tanto del sistema operativo como del software utilizado.

b. En los equipos de escritorio propiedad de la Corporación, la conexión a la red por medio de WIFI permanece deshabilitada por defecto. Solo se habilita en casos justificados, cuando existan limitaciones físicas que impidan la conexión por cable, previa autorización del Grupo TICS.

c. Para los dispositivos móviles que no pertenecen al inventario de activos fijos de la Corporación, no se permite la conexión directa a la infraestructura tecnológica corporativa. Estos dispositivos únicamente pueden acceder a la red Wi-Fi destinada para visitantes.

d. Para conectarse a la red de visitantes, los dispositivos completan el registro en el portal cautivo y obtienen la aprobación correspondiente. El acceso es válido por un periodo máximo de veinte (20) días, tras el cual se realiza nuevamente el proceso de registro para renovar la conexión.

### 2.5.5 Gestión De Contraseñas

Con el fin de reducir el riesgo de accesos no autorizados a los recursos tecnológicos de la Corporación, se establecen los siguientes lineamientos para la creación, gestión y protección de contraseñas:

#### 2.5.5.1 Requisitos Generales De Seguridad

a. Las contraseñas deben ser robustas y contener una combinación de letras mayúsculas y minúsculas, números y al menos un carácter especial.

b. No se deben utilizar contraseñas comunes o fácilmente adivinables, tales como combinaciones numéricas simples (ej.: “12345”), secuencias de letras (ej.: “abcd”) o palabras relacionadas con la Corporación o con información personal fácilmente accesible (nombres, fechas de nacimiento, etc.).

c. Las contraseñas no deben ser anotadas en lugares accesibles o inseguros (ej.: notas adhesivas visibles), ni almacenadas de forma no protegida en dispositivos electrónicos.

d. Las contraseñas proporcionadas temporalmente o por defecto (por fabricantes o administradores) deben cambiarse obligatoriamente en el primer inicio de sesión, garantizando que cumplan los criterios de seguridad establecidos.

e. No se puede reutilizar ninguna de las últimas tres contraseñas anteriores.

#### 2.5.5.2 Parámetros Específicos Por Sistema

a. Directorio Activo, equipo de cómputo, mesa de servicios, correo electrónico corporativo y la suite de Microsoft 365:

- Longitud mínima: 9 caracteres
- Longitud máxima: 15 caracteres
- Frecuencia de cambio: cada 45 días

b. ERP SAP:

- Longitud mínima: 8 caracteres
- Longitud máxima: 40 caracteres
- Frecuencia de cambio: cada 30 días

c. SuccessFactors:

- Longitud mínima: 8 caracteres
- Longitud máxima: 18 caracteres
- Frecuencia de cambio: cada 30 días

#### 2.5.5.3 Uso, Manejo Y Responsabilidades

a. Las contraseñas deben cambiarse dentro de los plazos establecidos para evitar problemas de acceso y garantizar la seguridad de los recursos tecnológicos.

b. Las contraseñas no deben anotarse en lugares accesibles o inseguros (como notas adhesivas, papeles visibles o archivos electrónicos sin protección).

c. Los usuarios son responsables de mantener la confidencialidad de sus credenciales de acceso y no deben compartirlas con otras personas.

d. Ante cualquier sospecha de compromiso o acceso no autorizado, deben cambiarla de inmediato y notificar al Grupo TICS.

e. Se debe evitar reutilizar contraseñas corporativas en servicios personales o plataformas no autorizadas

f. No se deben compartir contraseñas mediante medios inseguros como correos electrónicos, mensajería instantánea o documentos no cifrados

g. En caso de ausencia prolongada del usuario (vacaciones, licencias o retiro), las contraseñas asociadas a sus accesos se resetean o deshabilitan temporalmente.

#### 2.5.5.4 Autenticación Multifactor (MFA)

a. La autenticación multifactor (MFA) se aplica al correo electrónico, aplicaciones de Microsoft y a cualquier otro sistema o aplicación que lo permita, proporcionando una capa adicional de seguridad.

## 2.6 CRIPTOGRAFÍA

En cumplimiento de la Política General de Seguridad y Privacidad de la Información, la Corporación implementa herramientas de cifrado con el fin de proteger la confidencialidad, integridad y disponibilidad de la información. Por lo anterior, se establecen los siguientes lineamientos:

a. El Grupo TICS determina los equipos, usuarios o procesos a los cuales se instala o aplican controles criptográficos adicionales, según se requiera.

b. Las claves criptográficas se gestionan de forma segura, abarcando su generación, almacenamiento, distribución, uso y revocación, conforme a buenas prácticas de seguridad.

c. No se permite el uso de mecanismos criptográficos no autorizados ni herramientas de cifrado desarrolladas por terceros sin la validación y aprobación previa del Grupo TICS.

## 2.7 SEGURIDAD FÍSICA Y DEL ENTORNO

En cumplimiento de la Política General de Seguridad y Privacidad de la Información, y con el fin de prevenir accesos no autorizados, daños o interferencias que puedan afectar la infraestructura

tecnológica de la Corporación, se establecen controles destinados a proteger físicamente los recursos tecnológicos y de información, garantizando su confidencialidad, integridad y disponibilidad.

### 2.7.1 Áreas Seguras

Con el fin de controlar y restringir el acceso físico a espacios que albergan activos críticos como los Data Centers y centros de cableado, así como salvaguardar la información y las instalaciones contra accesos no autorizados, daños, pérdidas o interferencias, se establecen los siguientes lineamientos:

a. El acceso físico al Data Center principal, sus alternos y a los centros de cableado lo autoriza el Grupo TICS y se restringe únicamente al personal expresamente autorizado. Estas áreas permanecen cerradas con llave en todo momento, y cualquier ingreso se justifica y registra debidamente.

b. El ingreso de proveedores o visitantes se restringe. Cuando es necesario, están acompañados por personal del Grupo TICS durante toda su permanencia. En la sede de CAMAN, donde no hay presencia permanente del Grupo TICS, el acompañamiento lo realiza el Técnico Logístico o el Programador de Mantenimiento Aeronáutico, quienes están autorizados para acceder al Data Center y brindar este acompañamiento.

c. Los privilegios de acceso físico se modifican o revocan de forma inmediata ante cualquier cambio de funciones o desvinculación del personal autorizado.

d. El Grupo Administrativa es responsable de garantizar las condiciones físicas y medioambientales necesarias para el funcionamiento adecuado de los recursos tecnológicos alojados en estas áreas.

e. Las luces deben permanecer apagadas cuando no haya personal dentro del Data Center.

f. Cualquier solicitud de acceso excepcional a las áreas seguras requiere justificación y es evaluada y aprobada por la Coordinación del Grupo TICS.

g. Se siguen los lineamientos de control de acceso físico y seguridad establecidos por el Grupo Administrativa (Seguridad Aeroportuaria)

### 2.7.2 Seguridad De Equipos Y Dispositivos Móviles

Con el fin de prevenir accesos no autorizados, daños físicos o pérdida de información en los equipos tecnológicos, tanto dentro como fuera de las instalaciones, se establecen los siguientes lineamientos para su protección:

#### 2.7.2.1 Seguridad De Equipos

a. Los equipos de cómputo y demás dispositivos tecnológicos deben ubicarse en lugares seguros, protegidos de accesos no autorizados, condiciones ambientales adversas o riesgos físicos.

b. Cuando los equipos no estén en uso, deben apagarse o bloquearse, especialmente si están ubicados en áreas de acceso compartido, con el fin de prevenir accesos no autorizados o uso indebido.

c. Con el propósito de optimizar el consumo energético y prolongar la vida útil de los equipos, los computadores se apagan automáticamente a las 21:00 horas. Si se requiere continuar trabajando después de esta hora, el usuario debe enviar una solicitud formal por los medios establecidos, incluyendo la justificación correspondiente y el número de activo fijo del equipo.

d. A los usuarios se les proporciona una contraseña para el acceso al servicio de impresión, con el fin de garantizar el uso controlado, seguro y trazable de este recurso. Esta contraseña es personal e intransferible, y su confidencialidad debe ser preservada por el usuario.

e. El acceso a los equipos de cómputo se restringe exclusivamente al usuario al que se le ha asignado formalmente. En caso de requerir el uso de un equipo diferente, el responsable del equipo solicita la habilitación a través de los canales establecidos, adjuntando la justificación y el acta de activos fijos correspondiente. En situaciones de emergencia o casos excepcionales, el jefe, gerente o coordinador del grupo autoriza el acceso y presentan la justificación del caso.

f. El personal debe reportar cualquier daño físico, anomalía o pérdida de equipos al Grupo Administrativa y al Grupo TICS de manera inmediata.

#### 2.7.2.2 Seguridad De Los Dispositivos Móviles

a. Los dispositivos móviles tales como computadores portátiles y tabletas corporativas deben contar con medidas de protección física y lógica, como el uso de contraseñas de acceso, cifrado de disco y bloqueo automático tras períodos de inactividad.

b. El uso de dispositivos móviles para acceder a información institucional debe realizarse únicamente a través de redes seguras. Está prohibido el uso de redes Wi-Fi públicas no confiables sin medidas de protección como VPN corporativa.

c. Los dispositivos móviles deben mantenerse bajo supervisión directa del usuario cuando estén fuera de las instalaciones. No deben dejarse sin vigilancia en lugares públicos, vehículos u oficinas abiertas sin las debidas medidas de seguridad.

d. En caso de pérdida, robo o compromiso de un dispositivo móvil, el usuario debe notificar inmediatamente al Grupo Administrativa y al Grupo TICS para aplicar las acciones correctivas correspondientes.

e. Está prohibida la instalación de aplicaciones o software no autorizados en los dispositivos móviles corporativos, así como el uso compartido del equipo con personas ajenas a la Corporación.

## 2.8 SEGURIDAD DE LAS OPERACIONES

En cumplimiento de la Política General de Seguridad y Privacidad de la Información y con el fin de garantizar la seguridad, disponibilidad y eficiencia de los recursos tecnológicos que respaldan las operaciones de la Corporación, se establecen lineamientos para la implementación de controles operativos, orientados a proteger la confidencialidad, integridad y disponibilidad de la información.

### 2.8.1 Gestión De Cambios

Todo cambio que afecte los sistemas, servicios, infraestructura tecnológica o configuraciones críticas debe realizarse de manera controlada, minimizando los impactos sobre la seguridad, disponibilidad y funcionamiento de los servicios.

Los cambios deben cumplir con los siguientes criterios:

a. Antes de su implementación, cada cambio debe ser evaluado en términos de su impacto técnico, funcional y de seguridad.

b. Todo cambio debe contar con una aprobación documentada por parte de los responsables designados.

c. Los cambios deben quedar registrados en la herramienta o formato definido por el Grupo TICS, que permita su trazabilidad y seguimiento.

d. Cuando aplique, los cambios deberán probarse en entornos controlados antes de su puesta en producción, con el fin de identificar fallos o impactos no previstos. Se deberán considerar las recomendaciones de seguridad emitidas por fabricantes o proveedores. Además, estos cambios

deben ejecutarse, cuando sea posible, en horarios que minimicen el impacto sobre los servicios corporativos.

e. En caso de que un cambio afecte la disponibilidad o el funcionamiento de los recursos tecnológicos, los usuarios involucrados deben ser notificados previamente.
f. Todo cambio significativo debe ser revisado posteriormente para verificar su efectividad y detectar posibles desviaciones o fallos.

### 2.8.2 Protección Frente A Software Malicioso Y Ciberataques

Con el fin de proteger la infraestructura tecnológica de la Corporación frente a amenazas como virus, ransomware, spyware, ataques de fuerza bruta, suplantación, denegación de servicio y otros tipos de software malicioso o ciberataques, se establecen los siguientes lineamientos:

a. Todos los equipos corporativos deben contar con soluciones de seguridad actualizadas (antivirus, antimalware, firewall u otras herramientas de protección), gestionadas de forma centralizada por el Grupo TICS.

b. El sistema operativo, las aplicaciones y las herramientas de seguridad, especialmente las soluciones antivirus, antimalware, antispam y antispyware, deben mantenerse actualizadas conforme a las recomendaciones del fabricante para mitigar vulnerabilidades.

c. Se fomenta la concientización de los usuarios mediante campañas, capacitaciones y recomendaciones periódicas sobre ciberseguridad, con el fin de que puedan identificar los riesgos a los que están expuestos y saber cómo reaccionar ante ellos.

d. Los usuarios no deben contar con privilegios de administración, salvo autorización expresa. La instalación de software está restringida y debe ser aprobada por el Grupo TICS.

e. Se implementa el monitoreo continuo de la red y de los sistemas para detectar comportamientos anómalos, accesos no autorizados o indicios de código malicioso.

f. Es responsabilidad del personal reportar inmediatamente al Grupo TICS cualquier actividad sospechosa o incidente de seguridad, con el fin de que se activen las medidas de control correspondientes frente a amenazas o ciberataques potenciales.

### 2.8.3 Copias de Respaldo Y Restauración

Con el fin de garantizar la disponibilidad, la integridad y la recuperación de la información ante eventos de pérdida, daño, corrupción o incidentes de seguridad, se establecen y mantienen procedimientos formales para la realización de copias de respaldo y su posterior restauración. Estos lineamientos

buscan asegurar la continuidad de los servicios tecnológicos, así como la protección de la información crítica que respalda la operación de la Corporación.

#### 2.8.3.1 Copias De Respaldo

Con el fin de garantizar la disponibilidad y recuperación de la información crítica, se establecen los siguientes lineamientos para la realización y gestión de las copias de respaldo, tanto a nivel centralizado como a nivel de usuario:

Se deben realizar copias de respaldo periódicas de la información crítica, de acuerdo con la frecuencia definida por el Grupo TICS, considerando el nivel de criticidad y sensibilidad de los datos.

a. El Grupo TICS lleva a cabo copias incrementales diarias de los servidores locales y virtuales utilizando la herramienta Veeam Backup. Esta herramienta está configurada para enviar notificaciones automáticas al correo corporativo del personal del Grupo TICS, incluyendo un informe detallado sobre la ejecución de la copia de seguridad, el cual se verifica diariamente. La programación de estas copias de respaldo se detalla a continuación:

b. El Grupo TICS lleva a cabo copias incrementales diarias de los servidores locales y virtuales utilizando la herramienta Veeam Backup. Esta herramienta está configurada para enviar notificaciones automáticas al correo corporativo del personal del Grupo TICS, incluyendo un informe detallado de la ejecución, el cual debe ser verificado diariamente. La programación de estas copias de respaldo se detalla a continuación:

| Nombre Servidor | Tipo Backup | Hora Programa |
|---|---|---|
| **VM-SRVAD365** | Hyper-V Backup | 10:00 pm |
| **VM-SRVDC04** | Hyper-V Backup | 1:00 am |
| **VM-SRVFSFD** | Hyper-V Backup | 1:00 am |
| **VM-SRVISODB** | Hyper-V Backup | 10:10 pm |
| **VM-SRV-PLM** | Hyper-V Backup | 10:30 am |
| **VM-SRV_DDOC** | Hyper-V Backup | 12:30 pm<br>8:00 pm |
| **VM-SRV-LNXDDOC** | Hyper-V Backup | 12:30 pm<br>8:00 pm |
| **VM-SRV-PRINT** | Hyper-V Backup | 1:00 am |
| **VM-SRV-SDPLUS** | Hyper-V Backup | 12:00 pm |
| **VM-CL.UMVA1** | Hyper-V Backup | 2:00 am |
| **VM- CL.UMVA1** | Hyper-V Backup | 2:10 am |
| **SRV-FS01** | Image Backup | 12:30 am |

| | | |
|---|---|---|
| **SRV-20162** | Image Backup | 12:00 am |
| **SRV-2016** | Image Backup | 12:50 am |
| **SRVDCAMAN** | Image Backup | 2:00 am |

*Tabla 1 Programación copias de respaldo servidores virtuales*

c. Las copias de respaldo del ERP SAP son realizadas por la empresa proveedora del servicio de hosting, la cual entrega mensualmente una copia en medio físico con el respaldo completo correspondiente al mes vencido. Adicionalmente, se cuenta con un servidor de respaldo asignado a la Corporación, el cual contiene una réplica de la información de producción, garantizando la continuidad del servicio en caso de contingencia. Las copias de respaldo de la base de datos y los logs se programan de lunes a domingo, conforme a la programación detallada a continuación:

| Ambiente | Lunes | Martes | Miércoles | Jueves | Viernes | Sábado | Viernes |
|---|---|---|---|---|---|---|---|
| **Productivo** | Database | Database | Database | Database | Database | Database | Database |
| | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) |
| **Desarrollo** | | Database | | Database | | | |
| | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) |
| **Calidad** | | | | | Database | | |
| | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) |
| **Solman** | Database | Database | Database | Database | Database | Database | Database |
| | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) | Logs (3) |

*Tabla 2 Programación copias de respaldo ERP SAP*

d. Los respaldos se almacenan en medios o entornos seguros, separados lógica y/o físicamente de los sistemas de producción, bajo controles de acceso que garantizan la protección de la información.

e. El acceso a las copias de respaldo está restringido exclusivamente al personal autorizado, conforme a los perfiles de acceso definidos por el Grupo TICS.

f. Las configuraciones de los servidores deben ser revisadas y actualizadas periódicamente para asegurar la correcta ejecución de los procesos de respaldo.

g. En caso de que una copia de respaldo no pueda realizarse por motivos técnicos, como fallas en la infraestructura de almacenamiento o en la red, se aplica una excepción temporal hasta la resolución del incidente, sin comprometer la seguridad ni la disponibilidad de la información.

h. Se debe realizar una verificación periódica de la integridad de las copias de respaldo, con el fin de asegurar que los datos no se encuentren dañados o corrompidos.

i. Las copias de respaldo deben conservarse durante el período definido por las normas legales, las políticas internas o las necesidades operativas de la Corporación.

j. En caso de transición entre herramientas o plataformas de respaldo, las políticas de respaldo se adaptan temporalmente durante el proceso de migración, garantizando siempre la continuidad y seguridad de las copias de seguridad.

k. A los usuarios con cuenta Microsoft 365 se les proporciona acceso al servicio OneDrive Corporativo, con 1 TB de almacenamiento en la nube, como herramienta oficial para realizar copias de respaldo de su información digital.

l. Para los usuarios que cuentan con una cuenta tipo Quiosco de Exchange Online o que no disponen de una cuenta Microsoft 365 asignada, se asignará un espacio de almacenamiento de hasta 20 GB en la ubicación designada por el Grupo TICS.

m. Los usuarios deben cumplir con los lineamientos definidos en el apartado correspondiente a OneDrive, relacionados con la sincronización y respaldo automático de archivos.

n. Cada usuario es responsable de realizar el respaldo de la información que no se encuentre dentro de las carpetas sincronizadas, de acuerdo con la criticidad de los datos: diariamente para información crítica, semanalmente para información de menor frecuencia de actualización y mensualmente para información estática o no crítica.

o. En caso de requerir asistencia técnica para la realización de la copia de respaldo, el usuario debe realizar la solicitud al Grupo TICS a través de los canales establecidos.

p. El jefe, director o coordinador de grupo puede solicitar por los canales establecidos, la realización de una copia de respaldo de la información digital correspondiente al personal a su cargo.

q. En caso de retiro de personal, el jefe, director o coordinador de grupo es el responsable de verificar y recibir la copia de respaldo de la información del usuario, incluyendo los archivos almacenados en el equipo de cómputo, OneDrive y correo electrónico.

r. El usuario puede realizar una copia local de su correo electrónico, siguiendo el instructivo “I-7-00-004 Backup correo electrónico".

s. Las copias de respaldo deben contener exclusivamente información necesaria para el cumplimiento de funciones corporativas. No deben incluir archivos personales ni contenidos no autorizados como música, fotos o videos ajenos a la actividad corporativa.

t. El Grupo TICS no se responsabiliza por la pérdida de información que no haya sido respaldada de acuerdo con los lineamientos establecidos en este documento o en las herramientas oficiales dispuestas para tal fin.

#### 2.8.3.2 Restauración

Con el fin de garantizar la recuperación efectiva de la información ante incidentes, fallas o desastres, se establecen los siguientes lineamientos:

a. La restauración de los datos debe seguir un orden de prioridad establecido, comenzando con los sistemas y aplicaciones críticos para el funcionamiento de la Corporación.

b. El Grupo TICS es responsable de coordinar y ejecutar los procesos de restauración para los respaldos que tenga a cargo, así como de documentar los resultados correspondientes. En el caso del ERP SAP, la empresa prestadora del servicio de hosting es la encargada de ejecutar el proceso de restauración cuando se presenten fallas o desastres, garantizando la estabilidad del sistema.

c. Los procedimientos de restauración deben probarse periódicamente para verificar la integridad de los datos y la efectividad del proceso de recuperación.

d. Para la realización de las pruebas, se seleccionan aleatoriamente copias de respaldo, con el fin de validar que los datos puedan recuperarse de manera efectiva y que los procedimientos establecidos sean adecuados.

e. Las pruebas de restauración deben realizarse en un servidor específico destinado exclusivamente a este fin, de manera que no afecten los sistemas de producción.

f. Durante las pruebas se debe verificar tanto la integridad como la disponibilidad de los datos restaurados. Cualquier discrepancia o problema identificado deberá ser atendido de forma inmediata.

g. Después de cada prueba, se debe generar un registro detallado del proceso y sus resultados.

h. Los resultados obtenidos deben ser revisados y evaluados periódicamente. En caso de identificar patrones de fallos, se deben implementar las mejoras correspondientes en los procedimientos de respaldo y restauración.

i. En caso de que una restauración no pueda realizarse correctamente, el Grupo TICS aplica las medidas correctivas necesarias y escala el incidente a los niveles superiores de soporte, si corresponde.

### 2.8.4 Control De Software

Con el fin de mantener la seguridad, disponibilidad y cumplimiento normativo en el uso de software, además de controlar y prevenir riesgos derivados de la instalación o uso no autorizado de programas, se establecen los siguientes lineamientos:

a. Todo software utilizado en los equipos y sistemas corporativos debe contar con una licencia válida, estar autorizado y alinearse con las necesidades operativas de la Corporación.

b. La instalación, actualización o desinstalación de software en los equipos corporativos la realizada o autoriza exclusivamente el Grupo TICS, conforme a los estándares de seguridad, licenciamiento y compatibilidad técnica establecidos.

c. Los usuarios no tienen privilegios para instalar software en sus dispositivos sin autorización previa. En caso de requerir una aplicación específica, deben realizar una solicitud formal mediante los medios definidos por el Grupo TICS.

d. El Grupo TICS es responsable de administrar el software y autoriza a otras dependencias a gestionarlo cuando es necesario. El software no debe ser copiado, suministrado a terceros ni utilizado para fines personales sin autorización expresa.

e. El Grupo TICS mantiene un inventario actualizado de los programas instalados en los equipos corporativos, así como de las licencias asociadas, garantizando el cumplimiento legal y técnico.

f. Se realizan revisiones periódicas para detectar software no autorizado o desactualizado. En caso de identificarse aplicaciones que no cumplan con los lineamientos establecidos, se desinstalan.

g. El Grupo TICS gestiona las actualizaciones y parches de seguridad, evalúa los riesgos asociados y asegura la estabilidad operativa posterior a cada actualización.

h. El control de actualizaciones se realiza mediante una herramienta tecnológica destinada a validar los parches de los fabricantes antes de ser implementados en los equipos corporativos.

i. El Grupo TICS concede accesos temporales y controlados a los proveedores para realizar actualizaciones o tareas de mantenimiento, supervisa y registra las sesiones como evidencia de los ajustes realizados.

j. El uso de software de código abierto o gratuito es evaluado previamente por el Grupo TICS, quien verifica que no represente riesgos de seguridad ni incumpla condiciones de licenciamiento.

k. Cuando se detecta software potencialmente malicioso o sospechoso, el Grupo TICS procede con su aislamiento, análisis y eliminación.

### 2.8.5 Gestión De Incidentes

Con el fin de minimizar el impacto de los incidentes de seguridad que puedan afectar la confidencialidad, integridad o disponibilidad de la información y los servicios tecnológicos, se establecen los siguientes lineamientos:

a. Todo incidente o actividad sospechosa relacionada con la seguridad de la información y los servicios tecnológicos debe ser reportado de manera inmediata al Grupo TICS a través de los canales establecidos.

b. El Grupo TICS es responsable de coordinar la atención de los incidentes, incluyendo su clasificación, análisis, contención, recuperación y registro.

c. Los incidentes se categorizan según su tipo, nivel de severidad y alcance, para establecer prioridades de atención y definir los tiempos de respuesta.

d. Para el tratamiento de los incidentes se activan procedimientos de contingencia o se escala el caso a instancias superiores de soporte o gestión, de acuerdo con la criticidad del evento.

e. Todos los incidentes deben quedar registrados y documentados, incluyendo las acciones adoptadas, responsables y resultados, con el fin de mejorar la gestión futura.

### 2.8.6 Gestión De Vulnerabilidades

Con el fin de reducir los riesgos asociados a vulnerabilidades en los activos tecnológicos y prevenir posibles incidentes de seguridad, se establecen los siguientes lineamientos para su identificación, análisis, priorización y tratamiento:

a. El Grupo TICS es responsable de identificar y gestionar las vulnerabilidades que afecten a los sistemas, aplicaciones, dispositivos de red, equipos de usuario y demás componentes de la infraestructura tecnológica.

b. La identificación de vulnerabilidades se realiza mediante escaneos automáticos, revisiones técnicas, alertas de seguridad de fabricantes y proveedores, así como a través de reportes internos o externos.

c. Una vez identificadas, las vulnerabilidades deben ser analizadas y clasificadas de acuerdo con su nivel de criticidad, considerando el impacto potencial y la probabilidad de explotación.

d. El tratamiento de las vulnerabilidades debe contemplar acciones de remediación, mitigación o aceptación del riesgo, conforme a su clasificación y a las capacidades técnicas y operativas de la Corporación.
e. Las acciones correctivas aplicadas deben ser registradas y documentadas, manteniendo trazabilidad de los hallazgos, análisis y medidas adoptadas.

f. Se promueve la actualización permanente de sistemas operativos, aplicaciones y firmware, conforme a las recomendaciones de los fabricantes, con el fin de reducir la exposición a vulnerabilidades conocidas.

g. Periódicamente se revisarán las políticas y procedimientos relacionados con la gestión de vulnerabilidades, para asegurar su efectividad y alineación con las mejores prácticas y amenazas emergentes.

## 2.9 MEDIOS DE ALMACENAMIENTO

En cumplimiento de la Política General de Seguridad y Privacidad de la Información, y con el fin de prevenir riesgos asociados al almacenamiento de información en medios físicos y electrónicos, se establecen lineamientos orientados a proteger la confidencialidad, integridad y disponibilidad de la información corporativa.

### 2.9.1 Almacenamiento Removible

Con el fin de minimizar los riesgos que representan los medios de almacenamiento removible en términos de seguridad cibernética, se implementan los siguientes lineamientos:

a. El uso de medios de almacenamiento removible como memorias USB, discos duros portátiles, tarjetas SD, entre otros, está restringido en todos los equipos de cómputo corporativos.

b. Los puertos destinados a la conexión de medios de almacenamiento removible están bloqueados, con el propósito de evitar la transferencia de software malicioso que pueda comprometer la seguridad de la infraestructura tecnológica de la Corporación.

c. En casos excepcionales, cuando se requiera el uso de medios removibles por razones justificadas relacionadas con el core del negocio, se realiza una solicitud formal a la

Vicepresidencia Administrativa. Esta debe contar con el visto bueno de la Coordinación del Grupo TICS y está sujeta a evaluación y aprobación.

d. La transferencia de información desde y hacia dispositivos removibles se gestiona a través del Grupo TICS, mediante los canales establecidos. Los datos se almacenan en una carpeta de red para su control.

### 2.9.2 Almacenamiento En Red

Con el fin de regular el uso y manejo del almacenamiento conectado en red (NAS), se establecen los siguientes lineamientos:

a. La unidad QNAP, gestionada por el Grupo TICS, es el medio autorizado de almacenamiento en red donde se aloja información corporativa.

b. La creación, modificación o eliminación de carpetas compartidas debe ser solicitada formalmente al Grupo TICS y está sujeta a criterios operativos.

c. El acceso a las carpetas compartidas está restringido y se asigna según el grupo al que pertenece el usuario.

d. En caso de requerir acceso a una carpeta distinta a la asignada por grupo, se debe realizar una solicitud formal mediante los canales establecidos. El Grupo TICS gestiona la autorización con el propietario de la carpeta antes de conceder el acceso.

e. Las carpetas de escáner tienen un uso temporal y no cuentan con respaldo. La información allí contenida debe trasladarse oportunamente a la carpeta asignada a cada dependencia, la cual sí dispone de copia de seguridad.

f. El Grupo TICS realiza monitoreos periódicos del uso de los recursos compartidos y del cumplimiento de los lineamientos establecidos.

g. La unidad QNAP también se emplea como uno de los medios de respaldo de la información corporativa.

h. Los respaldos de la información almacenada en red se gestionan conforme a los lineamientos establecidos en el numeral de Copias de respaldo y restauración.

### 2.9.3 Almacenamiento En La Nube

Con el fin de proteger la información corporativa y garantizar su correcta gestión en entornos de almacenamiento en la nube, se establecen los siguientes lineamientos:

a. La herramienta oficial aprobada por la Corporación para el almacenamiento en la nube es Microsoft OneDrive, disponible para los usuarios de Microsoft 365. Esta permite acceder, sincronizar y compartir archivos de manera segura y en tiempo real.

b. En cada equipo corporativo, se configura OneDrive para sincronizar automáticamente las carpetas Escritorio, Documentos e Imágenes, utilizando la última versión estable de la aplicación.

c. En caso de reinstalación del sistema operativo, el Grupo TICS se encarga de reconfigurar OneDrive en el perfil del usuario, asegurando la sincronización de las carpetas predeterminadas mencionadas.

d. Para respaldar información adicional a las carpetas predeterminadas, los usuarios pueden solicitar soporte al Grupo TICS mediante los canales establecidos.

e. La sincronización de archivos se realiza de forma continua y automática. OneDrive conserva copias incrementales y versionadas, permitiendo la recuperación ante errores o cambios no deseados, y ofreciendo una capa adicional de protección frente a la pérdida de datos.

f. Los usuarios deben verificar al menos una vez por semana que la sincronización de OneDrive se esté ejecutando correctamente. En caso de fallos o errores, deben reportarlo de inmediato por los canales definidos.

g. El Grupo TICS realiza verificaciones periódicas sobre el estado de sincronización en los equipos y atiende de forma oportuna cualquier novedad detectada.

h. Es responsabilidad del usuario aplicar los controles de acceso adecuados a los archivos compartidos, garantizando que solo las personas autorizadas puedan visualizar, editar o compartir la información.

i. Se prohíbe el uso de servicios de almacenamiento en la nube que no estén debidamente controlados y autorizados por el Grupo TICS.

## 2.10 SEGURIDAD DE LAS COMUNICACIONES

En cumplimiento de la Política General de Seguridad y Privacidad de la Información, y con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información durante su transmisión a través de redes internas o externas, se establecen los siguientes lineamientos:

a. Las redes internas de la Corporación están protegidas mediante tecnologías de seguridad como firewalls, sistemas de detección de intrusos (IDS) y mecanismos de control de acceso, con el fin de prevenir accesos no autorizados.

b. Las redes inalámbricas corporativas cuentan con métodos de autenticación robustos que garantizan la conexión únicamente de dispositivos autorizados.

c. La red interna está segmentada y controlada, permitiendo el acceso únicamente a usuarios y dispositivos autorizados, de acuerdo con sus funciones y necesidades específicas.

d. Los servicios, puertos y protocolos innecesarios en las redes de datos deben ser deshabilitados, con el fin de reducir riesgo de exposición a posibles amenazas.

e. Se implementan mecanismos de monitoreo del tráfico de red para identificar actividades anómalas o no autorizadas que puedan representar riesgos para la seguridad de la información.

f. Los dispositivos de red, como switches, routers y firewalls, deben ser configurados siguiendo buenas prácticas de seguridad y su gestión está restringida al personal autorizado del Grupo TICS.

g. Las comunicaciones con terceros, incluidos proveedores y clientes, deben realizarse a través de canales seguros y previamente acordados, garantizando la protección de la información intercambiada.

## 2.11 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

En cumplimiento de la Política General de Seguridad y Privacidad de la Información, y con el fin de asegurar que los sistemas de información adquiridos, personalizados o desarrollados por terceros cumplan con los principios de confidencialidad, integridad y disponibilidad, así como con los objetivos corporativos, se establecen los siguientes lineamientos:

a. Todo proceso de adquisición, desarrollo o modificación de sistemas de información debe incluir el análisis de requisitos de seguridad desde su etapa de planeación, asegurando que los controles necesarios sean definidos e implementados desde el diseño.

b. Las dependencias que requieran la adquisición o adecuación de sistemas de información deben informar al Grupo TICS con el fin de revisar los aspectos técnicos, de seguridad, compatibilidad, escalabilidad y cumplimiento normativo, así como su alineación con la arquitectura tecnológica corporativa.

c. Todo sistema adquirido o implementado debe contar con documentación técnica y funcional que incluya manuales de usuario, administración, y especificaciones de seguridad para facilitar su implementación, operación y mantenimiento.

d. Todo sistema de información debe contar con mecanismos de respaldo, trazabilidad de actividades y controles de acceso adecuados, de acuerdo con la sensibilidad de la información que gestione.
e. Antes de aplicar cualquier modificación o actualización relevante a un sistema de información, se debe conservar una copia de seguridad actualizada que permita su recuperación ante posibles fallos

f. Las actualizaciones, cambios o mejoras en los sistemas de información deben gestionarse mediante procedimientos controlados que incluyan planificación, evaluación y validación antes de su puesta en producción.

g. Las pruebas de nuevas funcionalidades o actualizaciones deben realizarse en ambientes distintos al de producción, para evitar afectaciones en el servicio o en la integridad de la información.

h. Todo lo sistema de información debe someterse a mantenimiento regular que contemple actualizaciones de seguridad, parches y ajustes necesarios para mitigar vulnerabilidades.

i. Todos los sistemas deben incorporar mecanismos de control de sesión que incluyan límite de tiempo de inactividad y opciones de cierre de sesión (logout) para evitar accesos no autorizados.

## 2.12 RELACIÓN CON LOS PROVEEDORES

En cumplimiento de la Política General de Seguridad y Privacidad de la Información, y con el fin de asegurar que los proveedores que prestan servicios tecnológicos o gestionan información corporativa actúen conforme a los principios de confidencialidad, integridad y disponibilidad, se establecen los siguientes lineamientos:

a. La contratación de servicios tecnológicos o de terceros que tengan acceso a activos de información deben incluir cláusulas contractuales específicas relacionadas con la protección de datos, niveles de servicio, confidencialidad, continuidad del servicio y responsabilidades en materia de seguridad de la información.

b. Todo proveedor que gestione o tenga acceso a información corporativa debe firmar un acuerdo de confidencialidad antes de iniciar cualquier actividad. Este acuerdo tiene vigencia durante toda la relación contractual y por un período de tres (3) años posteriores a su finalización.

c. Se deben establecer mecanismos de control y seguimiento para verificar el cumplimiento de los compromisos de seguridad por parte de los proveedores durante la vigencia del contrato.

d. Los accesos proporcionados a proveedores externos son temporales, limitados y autorizados formalmente. Estos accesos se revocan una vez finalizada la actividad o servicio.

## 2.13 GESTIÓN DE CONTINUIDAD DEL NEGOCIO

En cumplimiento de la Política General de Seguridad y Privacidad de la Información, y con el fin de preservar la confidencialidad, integridad y disponibilidad de la información ante eventos que puedan afectar la operación normal de los servicios tecnológicos, se establecen los siguientes lineamientos:

a. Se debe establecer mecanismos que garanticen la continuidad de los servicios tecnológicos críticos y la recuperación oportuna de la información ante incidentes que afecten su disponibilidad.

b. El Grupo TICS debe contar con un Plan de Continuidad Tecnológica orientado a la restauración de los servicios tecnológicos esenciales y a la protección de la infraestructura crítica de información.

c. Se debe definir y mantener actualizado un inventario de activos de información críticos, junto con la asignación de sus responsables, con el fin de priorizar su recuperación en caso de incidentes.

d. El Plan de Continuidad Tecnológica debe ser probado periódicamente para verificar su eficacia y realizar los ajustes necesarios que garanticen su operatividad ante eventos reales.

## 2.14 USO DE LOS RECURSOS TECNOLÓGICOS

En cumplimiento de la Política General de Seguridad y Privacidad de la Información, y con el fin de garantizar el uso adecuado, eficiente y seguro de los recursos tecnológicos dispuestos por la Corporación, se establecen los siguientes lineamientos:

a. Los recursos tecnológicos, tales como equipos de cómputo, software, redes, servicios de internet, correo electrónico y dispositivos móviles, deben ser utilizados exclusivamente para el desarrollo de las funciones asignadas, conforme a los fines corporativos.

b. Está prohibido el uso de los recursos tecnológicos para fines personales, actividades ilícitas, difusión de contenidos inapropiados o cualquier acción que represente un riesgo para la seguridad de la información o que afecte la reputación de la Corporación.

c. Los usuarios son responsables de proteger la información a la que acceden, evitando divulgar credenciales, compartir archivos sin autorización o ejecutar acciones que comprometan la seguridad la información o de la infraestructura tecnológica de la Corporación.

d. Se prohíbe el almacenamiento de credenciales en navegadores web o cualquier otro medio no autorizado, con el fin de preservar la seguridad de la información y evitar accesos no autorizados.

e. Los dispositivos tecnológicos deben mantenerse actualizados y protegidos mediante contraseñas seguras, bloqueo de pantalla y otras medidas de seguridad definidas por el Grupo TICS.

f. Solo el personal autorizado por el Grupo TICS puede realizar modificaciones, actualizaciones o reparaciones en los recursos tecnológicos, incluyendo tareas como destapar equipos, agregar o desconectar componentes, realizar instalaciones o configuraciones.

g. El personal del Grupo TICS solo presta soporte técnico sobre los recursos tecnológicos de propiedad de la Corporación.

h. Cada funcionario es responsable por los registros, modificaciones o actualizaciones realizadas a la información mediante su cuenta de usuario, así como de las consecuencias derivadas de su uso.

i. Al momento de la desvinculación laboral, el Grupo TICS revoca los accesos y desvincula de todos los dispositivos asociados a la cuenta Microsoft 365 del usuario, con el fin de salvaguardar la seguridad e integridad de la información corporativa.

### 2.14.1 Uso Adecuado De Internet

Con el fin de proteger la infraestructura tecnológica de la Corporación y minimizar los riesgos asociados al uso del servicio de Internet, se establecen los siguientes lineamientos:

a. El acceso a Internet está orientado al cumplimiento de funciones laborales, permitiendo únicamente la consulta, descarga y uso de contenidos relacionados con las actividades corporativas.

b. No está permitido el acceso a sitios web que contengan material inapropiado, malicioso o que representen riesgos para la seguridad de la información, tales como contenido explícito, plataformas de descarga no autorizadas, sitios que violen derechos de autor, promuevan apuestas, armas, explosivos o que atenten contra la integridad moral de las personas, las instituciones, las leyes vigentes o las directrices establecidas por la Corporación.

c. Se restringe el acceso a plataformas de streaming de audio y video, redes sociales, mensajería instantánea, videojuegos, tiendas en línea, así como a sitios con contenido para adultos, relacionados con alcohol, armas, explosivos, apuestas, loterías y otros sitios con fines

recreativos, salvo que sean estrictamente necesarios para el cumplimiento de funciones laborales específicas.

d. El uso de Internet debe realizarse de forma responsable, evitando la navegación en sitios que no estén relacionados con las funciones corporativas o que puedan comprometer la seguridad de la infraestructura tecnológica.

e. Está prohibido propagar intencionalmente virus, malware o cualquier tipo de código malicioso que pueda afectar la red corporativa.

f. En caso de requerir acceso a un sitio web específico no habilitado, la solicitud debe realizarse de manera formal a través de los canales establecidos, justificando la necesidad de acceso. La solicitud está sujeta a verificación, aprobación y habilitación por parte del Grupo TICS.

g. El Grupo TICS realiza monitoreo del tráfico de red con el fin de detectar comportamientos anómalos, prevenir incidentes de seguridad y verificar el cumplimiento de estos lineamientos.

### 2.14.2 Uso Adecuado Del Correo Electrónico

Con el fin de preservar la seguridad de la información y promover el uso responsable del correo institucional, se establecen los siguientes lineamientos:

a. El único servicio de correo electrónico autorizado para la transmisión y manejo de información corporativa es el proporcionado por el Grupo TICS, con el dominio @ciac.gov.co, el cual cumple con los requisitos técnicos y de seguridad establecidos, protegiendo así la red contra posibles ciberataques.

b. El correo electrónico corporativo debe utilizarse exclusivamente para el desarrollo de funciones laborales y la comunicación corporativa. No debe emplearse para asuntos personales ni para suscribirse a servicios o plataformas ajenas a las actividades de la Corporación.

c. Cada cuenta de correo es de uso personal e intransferible. El usuario asignado es responsable de su administración y no debe permitir que terceros la utilicen.

d. Los buzones de correo y toda la información contenida en ellos son propiedad exclusiva de la Corporación de la Industria Aeronáutica Colombiana - CIAC.

e. El uso del correo debe ser respetuoso y profesional. Se prohíbe el envío de mensajes con contenido ofensivo, difamatorio, discriminatorio o que atente contra la imagen de la Corporación o sus funcionarios.

f. La creación de cuentas de correo electrónico se realiza conforme a los lineamientos establecidos en el numeral de Gestión de Acceso A Usuarios y está sujeta a la disponibilidad de licencias.

g. El nombre de usuario se genera utilizando la inicial del primer nombre, punto, seguido del primer apellido (ejemplo: i.apellido@ciac.gov.co). En caso de duplicidad, se añade la inicial del segundo apellido. Pueden aplicarse excepciones por razones operativas o de registros ante entidades externas.

h. La cuenta se bloqueada tras tres intentos fallidos de inicio de sesión. Luego de cinco minutos, se reactiva automáticamente. Los intentos quedan registrados en el historial de inicio de sesión de Microsoft 365.

i. Los métodos de autenticación incluyen contraseña, número de celular, código SMS de un solo uso y Microsoft Authenticator. Esta configuración puede modificarse para fortalecer la seguridad, según sea necesario.

j. Todo el personal que utilice correo electrónico corporativo (Microsoft 365 o Quiosco de Exchange) debe instalar y configurar la aplicación Microsoft Authenticator para acceder a su cuenta, como medida de protección adicional.

k. Es responsabilidad de cada usuario mantener actualizados los datos de autenticación multifactor (MFA). En caso de pérdida de dispositivos o inconvenientes técnicos, se debe notificar al Grupo TICS de inmediato.

l. No está permitido el envío de correos masivos internos o externos, salvo por vicepresidentes, jefes, gerentes o coordinadores, o por personal expresamente autorizado. El envío está limitado a un máximo de dos personas por grupo.

m. Se prohíbe abrir enlaces o descargar archivos de correos sospechosos o de remitentes desconocidos. Ante cualquier duda, se debe informar al Grupo TICS.

n. El uso de correos electrónicos externos (Gmail, Hotmail, Yahoo, u otros.) está restringido, salvo autorización expresa del Grupo TICS y registro en la lista blanca del firewall. Se exceptúan de esta restricción los siguientes casos: Recepción y respuesta de PQRSF, verificación de autenticación para acceder a la administración del sitio web corporativo, administración de redes sociales corporativas y personal de soporte del Grupo TICS.

o. Los correos desde dominios externos están sujetos a verificación de contenido por parte del Grupo TICS, tanto para el envío como la recepción.

p. El personal en comisión, dentro o fuera del país, deben solicitar el acceso al correo corporativo mediante los canales establecidos, conforme al numeral Accesos Para El Personal En Comisión, en el apartado de Gestión de Accesos.

q. El Grupo TICS puede realizar copias de seguridad del correo corporativo en cualquier momento, sin previo aviso, así como restringir o suspender temporal o definitivamente el acceso a las cuentas, previa solicitud expresa de Presidencia, Vicepresidencias o del jefe, gerente o coordinador de grupo correspondiente.

r. El Grupo TICS monitorea el uso del correo corporativo, conforme a la normatividad vigente, para prevenir incidentes de seguridad y garantizar el cumplimiento de estos lineamientos.

### 2.14.3 Uso De Redes Sociales

Con el fin de proteger la imagen corporativa y garantizar una gestión responsable de la información publicada en medios digitales, se establecen los siguientes lineamientos:

a. El acceso y gestión de las redes sociales corporativas está restringido exclusivamente al Grupo de Comunicaciones. Ningún otro funcionario puede crear, administrar o publicar contenido en nombre de la Corporación a través de redes sociales, salvo autorización expresa de la Presidencia o Vicepresidencias.

b. El nombre, logotipo o cualquier elemento de identidad corporativa no debe utilizarse en redes sociales de manera que afecte la imagen, reputación o integridad de la Corporación. En caso de responder a comentarios negativos, debe mantenerse una postura respetuosa y coherente con los principios y valores corporativos.

c. En situaciones que involucren crisis comunicacional o comentarios negativos en redes sociales, únicamente el Grupo de Comunicaciones está autorizado para responder, tomar acciones y dirigir la estrategia de comunicación correspondiente.

d. Los funcionarios que utilicen redes sociales a título personal deben abstenerse de presentarse como voceros oficiales de la Corporación o divulgar información interna, confidencial o no autorizada. En sus publicaciones, deben actuar con responsabilidad y evitar emitir opiniones que puedan comprometer la imagen corporativa.

### 2.14.4 Pantalla Limpia

Con el propósito de proteger la información digital de la Corporación y prevenir accesos no autorizados, se deben seguir los siguientes lineamientos cuando los dispositivos no estén en uso o queden desatendidos:

a. Los usuarios deben cerrar sesión o bloquear el equipo con contraseña al ausentarse de su puesto de trabajo, incluso por períodos cortos.

b. Los equipos de cómputo se bloquean automáticamente tras un período máximo de tres (3) minutos de inactividad, como medida de control ante dispositivos desatendidos.

c. No debe permanecer visible en pantalla información confidencial o sensible sin supervisión, especialmente en espacios compartidos.

d. La documentación digital en curso debe guardarse en las ubicaciones autorizadas (como carpetas compartidas o OneDrive corporativo), evitando dejar archivos abiertos o sin guardar.

e. Los datos de acceso no deben ser anotados ni almacenados en lugares visibles o inseguros, como notas adhesivas, papeles o documentos accesibles a terceros.

f. En las sesiones remotas de servidores debe configurarse el cierre automático tras un período de inactividad, como mecanismo de seguridad.

## 2.15 SENSIBILIZACIÓN Y COMUNICACIÓN

Con el fin de fortalecer la cultura organizacional orientada a la seguridad de la información, seguridad digital y ciberseguridad, se desarrollarán acciones de sensibilización y comunicación dirigidas al personal de la Corporación. Estas actividades buscan fomentar el conocimiento y la apropiación de los lineamientos establecidos en el presente documento, así como promover buenas prácticas en el uso seguro de la información.

a. El Grupo TICS, en conjunto con el Grupo de Comunicaciones, son los encargados de diseñar y difundir contenidos informativos y campañas de sensibilización sobre el uso seguro y responsable de los recursos tecnológicos.

b. Las acciones incluyen capacitaciones virtuales o presenciales, boletines, mensajes en medios digitales internos, infografías, ejercicios prácticos de concienciación y otros recursos pedagógicos.

c. Los lineamientos establecidos en el presente documento se socializan al momento del ingreso del personal, como parte del proceso de inducción, y se refuerzan periódicamente a través de estrategias corporativas.

d. Todo el personal, incluidos contratistas, pasantes, aprendices y proveedores con acceso a los recursos tecnológicos o información de la Corporación, deben mantenerse informado sobre los

lineamientos vigentes y participar activamente en las actividades de sensibilización y comunicación programadas.

## 2.16 CUMPLIMIENTO

El cumplimiento de los lineamientos establecidos en este documento es obligatorio para todo el personal de la Corporación, incluidos contratistas, pasantes, aprendices y proveedores que tengan acceso a los recursos tecnológicos o a la información institucional. Estas disposiciones buscan garantizar la seguridad, integridad y confidencialidad de los activos de información, en concordancia con la normativa legal vigente y los compromisos contractuales adquiridos por la Corporación.

### 2.16.1 Cumplimiento De Requisitos Legales Y Contractuales

La Corporación de la Industria Aeronáutica Colombiana - CIAC en el marco de su compromiso con la seguridad y privacidad de la información, garantiza el cumplimiento de la legislación vigente, así como de los requisitos contractuales, normativos y regulatorios aplicables en materia de derechos de autor, propiedad intelectual, privacidad y protección de datos personales, transparencia y derecho de acceso a la información pública, así como cualquier otra normativa relacionada con la seguridad de la información.

#### 2.16.1.1 Derechos De Autor Y Propiedad Intelectual

Con el fin de asegurar el cumplimiento de las leyes de derechos de autor y de propiedad intelectual en el uso del software y demás recursos digitales, se establecen los siguientes lineamientos:

a. Adquirir software únicamente a través de fuentes confiables, asegurando su legalidad y que no se vulneren derechos de autor.

b. Verificar que todo software instalado en los recursos tecnológicos cuente con licencias válidas y vigentes, garantizando su autenticidad.

c. Implementar mecanismos de control para asegurar que no se exceda el número máximo de usuarios permitidos por las licencias adquiridas.

d. Implementar mecanismos de control que aseguren el cumplimiento de los términos de las licencias, incluyendo el número de usuarios permitidos.

e. Mantener un registro actualizado de las licencias adquiridas, y gestionar oportunamente su renovación o actualización.

f. Se prohíbe la instalación, uso o duplicación de software sin los derechos de uso correspondientes, en cumplimiento de la normativa de propiedad intelectual

#### 2.16.1.2 Protección De Datos Personales

La Corporación de la Industria Aeronáutica Colombiana – CIAC, en cumplimiento de la normativa vigente sobre tratamiento de datos personales, reconoce que estos son propiedad de los titulares y que solo ellos pueden decidir sobre su uso. Por tanto, su tratamiento se realiza exclusivamente para las finalidades autorizadas y bajo los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

El uso, recolección, almacenamiento, procesamiento y eliminación de datos personales debe cumplir con lo establecido en la **Resolución N° 013 del 25 de enero de 2023** "*Por medio de la cual se adopta la política para el tratamiento de datos personales, se designa y establecen las competencias del oficial de datos personales de la Corporación de la Industria Aeronáutica Colombiana S.A*.", así como con cualquier otra disposición legal o reglamentaria aplicable.

### 2.16.2 Revisiones De Seguridad Y Privacidad De La Información

Los lineamientos establecidos en el presente documento se revisan al menos una vez al año, o cuando se presenten situaciones que lo ameriten, tales como:

- Cambios en la aplicabilidad del documento.
- Materialización de riesgos o incidentes de seguridad.
- Identificación de oportunidades de mejora.
- Observaciones o hallazgos en auditorías.
- Cambios estructurales relevantes en la Corporación.
- Emisión de nuevas disposiciones legales o regulatorias aplicables.

Estas revisiones buscan asegurar la vigencia, pertinencia y aplicabilidad de los lineamientos en materia de seguridad y privacidad de la información.

Los ajustes que se deriven se formalizan mediante el procedimiento de control de cambios del SIGCA, tienen efecto a partir de su aprobación y se comunican oportunamente al personal y demás partes interesadas a través de los medios corporativos definidos.

### 2.16.3 Sanciones

El incumplimiento de los lineamientos de seguridad y privacidad de la información establecidos en este manual se considera una infracción que puede afectar la confidencialidad, integridad y disponibilidad de los datos gestionados por la Corporación. Las sanciones correspondientes pueden ser de carácter

disciplinario, contractual o legal, dependiendo de la naturaleza y gravedad de la falta, y se aplica conforme a la normativa interna y la legislación vigente.

Cada caso se analiza de manera individual, teniendo en cuenta sus circunstancias particulares, y se informa a las áreas competentes para la determinación y aplicación de las medidas que correspondan.

El Grupo TICS brinda acompañamiento técnico en la verificación de los incidentes, el análisis de causas y la recolección de evidencias, con el propósito de apoyar a las instancias responsables en la toma de decisiones.