TABLA DE CONTENIDO

INTRODUCCIÓN

Conscientes de que la seguridad informática se fundamenta en la existencia y aplicación de un conjunto de lineamientos que brindan orientaciones claras relativas a la seguridad y privacidad de la información, el Consejo Profesional Nacional de Ingeniería (COPNIA) presenta el Manual de Seguridad de la Información, como parte del compromiso de la entidad con los pilares fundamentales de confidencialidad, integridad y disponibilidad de la información.

El presente manual de seguridad de la información desarrolla las políticas y lineamientos que integran el Sistema de Gestión de Seguridad de la Información (SGSI), orientando el cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en el modelo de seguridad y privacidad de la información de la estrategia Gobierno en Línea (GEL) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, las cuales deben ser adoptadas por los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el COPNIA.

Cada uno de los numerales presentes en el documento son aplicables a todos los procesos de la Entidad, a la implementación de proyectos, intercambio de información con terceros, gestión de la información y a la operación diaria de las actividades propias del COPNIA.

1. OBJETO Y ALCANCE

1.1 OBJETO

Establecer los lineamientos que regulan la seguridad de la información en el Consejo Profesional Nacional de Ingeniería – COPNIA, con el fin de que sean conocidos y acatados por los funcionarios, contratistas, proveedores y demás terceros que desarrollen actividades, presten algún servicio o tengan algún tipo de relación con la entidad, con el propósito de mitigar el riesgo de pérdida, acceso, uso, divulgación, interrupción o destrucción no autorizada de información.

Nota: Para el desarrollo del Manual de Seguridad de la Información, se utilizó como referencia la Guía no.2 "Elaboración de la política general de seguridad de la información y privacidad de la información", Versión inicial 1.0.0 de 11 de mayo de 2016 del Ministerio de Tecnologías de la Información y las Comunicaciones, MinTIC.

1.2 ALCANCE

El Manual de Seguridad de la Información contiene los lineamientos generales para la implementación de un modelo de gestión de seguridad y privacidad de la información, a través de la identificación de responsabilidades y disposiciones generales en torno a la gestión de activos, el control de accesos, el no repudio, la privacidad y confidencialidad, la integridad, la disponibilidad del servicio y la información, el registro y la auditoría, la gestión de incidentes y las acciones de capacitación y sensibilización.

El Manual de Seguridad de la Información es aplicable a todos los procesos, así como a todos los aspectos administrativos, contractuales y de control que deben ser cumplidos por los funcionarios, supernumerarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el Consejo Profesional Nacional de Ingeniería – COPNIA.

La inobservancia de las disposiciones de este documento podrá dar lugar según corresponda, a la iniciación de las investigaciones y aplicación de las sanciones, de conformidad con las disposiciones legales vigentes.

2. MARCO INSTITUCIONAL

2.1 NATURALEZA DEL COPNIA

El Consejo Profesional Nacional de Ingeniería – COPNIA, creado mediante la Ley 94 de 1937, es la **entidad pública que tiene la función de controlar, inspeccionar y vigilar el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, en el territorio nacional**; de acuerdo con lo dispuesto en el Artículo 26 de la Constitución Política y en la Ley 842 de 2003 y demás normas complementarias y suplementarias, autorizando a nombre del Estado el ejercicio de una profesión que implica riesgo social, o suspendiendo el ejercicio profesional, previo la aplicación del debido proceso, a quienes se les compruebe la violación del Código de Ética o del correcto ejercicio de la profesión autorizada; esto último en su calidad de Tribunal de Ética de las profesiones tuteladas, por quejas interpuestas por la ciudadanía.

En razón de lo anterior, el COPNIA desarrolla su función mediante la expedición de cuatro herramientas legales a saber: **Matrícula Profesional**, para los ingenieros; **Certificado de Inscripción Profesional**, para profesionales afines y profesionales auxiliares; **Certificado de Matrícula**, para maestros de obra y **Permisos Temporales**, para profesionales graduados y domiciliados en el exterior que pretendan ejercer temporalmente en Colombia, de acuerdo con lo dispuesto en el artículo 23 de la Ley 842 de 2003.

Cuenta con una sede central de carácter nacional en la ciudad de Bogotá, D.C. y con 17 consejos regionales y seccionales que actúan como primera instancia en sendos Departamentos, en los que existen Facultades de Ingeniería o Instituciones de Educación Superior que otorgan títulos de ingeniero, de profesional afín o de profesional auxiliar, respectivamente, de las profesiones controladas por el COPNIA en virtud de lo dispuesto en la Ley 842 de 2003.

Al COPNIA lo conforman actualmente: la Junta Nacional de Consejeros (Art.26 de la Ley 435 de 1998 y Art.3 de la Ley 1325 de 2009) y 17 Juntas de consejos regionales y seccionales en cada uno de los departamentos del país en los que existen facultadas de ingeniería, integradas según lo dispuesto en el artículo 28 de la Ley 842 de 2003.

La expedición de la Ley 1325 de 2009, le otorgó nuevamente al COPNIA, la competencia para controlar e inspeccionar el ejercicio de las ingenierías: Agrícola, Forestal, Agronómica y Pesquera, así como de la Agronomía y de la Agrología, de sus profesiones Afines y de sus profesiones Auxiliares, ampliando a la vez la conformación de la Junta Nacional de Consejeros, con el Ministro de Agricultura o su delegado y el Presidente de uno de los gremios involucrados, elegido en Junta convocada por el COPNIA, para tal fin.

2.2 MISIÓN

Somos la autoridad pública encargada de velar por el buen ejercicio profesional de los ingenieros, profesionales afines y auxiliares, mediante la autorización, inspección, vigilancia y control, que se concreta con la administración del Registro Profesional, del Registro Único Nacional de Profesionales Acreditados y con la función de Tribunal de Ética Profesional.

2.3 VISIÓN

En el año 2026, seremos una entidad reconocida por la prestación del servicio con calidad y oportunidad, por el fortalecimiento de la relación con los profesionales inscritos en los Registros y con los demás grupos de interés, promoviendo la cultura ética en el ejercicio profesional, apoyados en el uso de tecnologías de la información, la gestión efectiva de las comunicaciones y el compromiso y responsabilidad de todos los funcionarios con el servicio a la ciudadanía.

3. TÉRMINOS Y DEFINICIONES

- **Disponibilidad:** Según [ISO/lEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

- **Integridad**: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo controlde sujetos obligados. (Ley 1712 de 2014, art 4)

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC27000).

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contieneinformación pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidadde tal.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservadosrespetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la instituciónque está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de2000, art 3)

- **ISO 27001**: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013 y tercera publicación en 2022.

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamientode datos personales (Ley 1581 de 2012, art 3)

- **BitLocker:** es una característica de cifrado de disco completo integrada en los sistemas operativos Windows, diseñada para proporcionar una capa adicional de seguridad a los datos almacenados en unidades de disco duro y dispositivos de almacenamiento extraíbles.

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Derechos de Acceso Privilegiado:** se refieren a los privilegios y autorizaciones especiales otorgados a usuarios dentro de un sistema o red, concediéndoles niveles de acceso más elevados de lo habitual. Estos derechos permiten a los usuarios realizar acciones y operaciones que van más allá de las funciones estándar, como la capacidad de modificar configuraciones críticas, acceder a información sensible o realizar cambios en el entorno tecnológico. La gestión cuidadosa de los Derechos de Acceso Privilegiado es esencial para garantizar la seguridad de la información, ya que un uso indebido o la explotación de estos privilegios pueden resultar en riesgos significativos de seguridad.

- **Encripción:** es un proceso de codificación de datos que transforma la información legible en un formato ilegible mediante el uso de algoritmos y claves, con el objetivo de proteger la confidencialidad y seguridad de la información durante su transmisión o almacenamiento.

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Matriz de Roles y Perfiles:** herramienta utilizada en la gestión de identidad y acceso para organizar y asignar de manera eficiente los roles y responsabilidades de los usuarios dentro de un sistema o una organización. Esta matriz proporciona una representación visual que relaciona los roles específicos con los perfiles de usuarios, detallando las funciones y privilegios asociados a cada uno. Al establecer esta estructura, se facilita la administración de la seguridad informática al definir claramente quién tiene acceso a qué recursos y funciones dentro de un sistema. Esta práctica no solo mejora la eficiencia en la asignación de permisos, sino que también fortalece la seguridad al garantizar que los usuarios tengan solo los privilegios necesarios para desempeñar sus funciones, siguiendo el principio del menor privilegio.

- **MFA:** Autenticación Multifactor, es una medida de seguridad avanzada que requiere que los usuarios proporcionen múltiples formas de verificación para acceder a sistemas, aplicaciones o datos. A diferencia de la autenticación tradicional basada en contraseñas, que se fundamenta en un solo factor (algo que el usuario sabe), la MFA agrega capas adicionales de seguridad al incorporar elementos como algo que el usuario posee (como un dispositivo móvil)

o algo inherente al usuario (como huellas dactilares o reconocimiento facial). Este enfoque fortalece significativamente la protección contra accesos no autorizados, ya que incluso si un elemento de autenticación se ve comprometido, otros factores adicionales siguen protegiendo el acceso. La MFA se ha convertido en una práctica estándar en la ciberseguridad, proporcionando una defensa robusta contra amenazas como el robo de contraseñas y el acceso no autorizado a sistemas críticos.

- **No repudio:** Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

- **RTO:** Tiempo de Recuperación Objetivo, es el período de tiempo máximo que una entidad establece como objetivo para restaurar sus operaciones normales después de un incidente o interrupción. Es la duración máxima que la organización puede permitirse estar fuera de servicio antes de que impacte negativamente en sus funciones críticas. Establecer un RTO proporciona una guía clara para la planificación y la implementación de estrategias de recuperación, permitiendo a la organización minimizar el tiempo de inactividad y recuperarse eficientemente de eventos no deseados.

- **RPO:** Significa Objetivo de Punto de Recuperación en inglés (Recovery Point Objective), se refiere al intervalo máximo de tiempo aceptable en el cual los datos pueden perderse durante un incidente o interrupción. En otras palabras, establece el punto en el tiempo al que una entidad está dispuesta a recuperarse después de un evento adverso, como un fallo del sistema o un desastre, indicando cuánta información puede permitirse perder sin afectar significativamente sus operaciones. Determinar un RPO efectivo es crucial para la planificación de la continuidad del negocio y la implementación de estrategias de respaldo y recuperación de datos.

- **Seguridad de la información:** Son todos los controles técnicos y metodológicos que permiten mitigar los riesgos a los que se expone la información en general.

- **SGSI:** Sistema de Gestión de Seguridad de la Información. Es el diseño, implantación, mantenimiento deun conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

- **TIC:** El término tecnologías de información y comunicación (TIC).

4. NORMATIVIDAD

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- Constitución Política de Colombia 1991. Artículo 20. Libertad de Información.
- Código Penal Colombiano - Ley 599 de 2000.
- Ley 679 de 2001- Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución
- Ley 906 de 2004, Código de Procedimiento Penal.
- Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 594 de 2000 - Ley General de Archivos.
- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
- Ley 1032 de 2006, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".

- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Ley 1712 de 2014, "De transparencia y del derecho de acceso a la información pública nacional".
- Ley 962 de 2005. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;"
- Ley 1150 de 2007. "Seguridad de la información electrónica en contratación en línea"
- Ley 1341 de 2009. "Tecnologías de la Información y aplicación de seguridad".
- Decreto 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008".
- Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".
- Decreto 1083 de 2015. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital.

5. LINEAMIENTO PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1 Organización para la seguridad de la información[1]

Los lineamientos relativos a la organización de la seguridad de la información, tales como conformación y objetivos de comités, funciones y responsabilidad, se encuentran definidos en la normativa asociada al Modelo Integrado de Planeación y Gestión del COPNIA.

Los Líderes funcionales son responsables de establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información del COPNIA, conforme a las funciones asignadas al área de desempeño. Los roles, funciones y responsabilidades deberán estar debidamente documentados y distribuidos, conforme a lineamientos establecidos para el control documental de la Entidad.

La Entidad cuenta con el Subcomité de Seguridad de la Información, el cual se encuentra conformado según resolución nacional que se encuentra en el link https://www.copnia.gov.co/transparencia/comites-copnia, donde el presente comité realiza el análisis de diferentes situaciones que impactan la seguridad de la información y la privacidad de los datos, realizando recomendaciones alineadas a las políticas de la seguridad de la información de la Entidad, para que estas sean avaladas por el Comité Institucional de Gestión y Desempeño.

5.2 Gestión de Activos[2]

A continuación, se relacionan las directrices que orientan a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de información.

5.2.1 Identificación de activos

Propiedad intelectual: El COPNIA es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios del COPNIA y los contratistas,

[1] Esta política tiene como finalidad establecer el subcomité de Seguridad de la Información.
[2] Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información

derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

Equipos de cómputo: Es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones nombrar los activos de cómputo del COPNIA, nomenclatura: CO más número de identificación único (placa de inventario), que permita la administración de su ubicación y asignación final a los usuarios responsables. Ejemplo: CO160300036. Para realizar la actividad, es necesario que el activo de cómputo cuente con placa de inventario asignado por el área Administrativa.

Gestión documental: de acuerdo con los criterios de administración documental del COPNIA, directrices para la creación y diseño de documentos, sistema de gestión de documentos electrónicos de archivo – SGDEA, mecanismos de autenticación y mecanismos de asignación de metadatos enfocados en el marco de la planeación que debe generar la entidad, los lineamientos de creación y actualización del registro de activos de información se rige por las definiciones del Programa de Gestión Documental de la Entidad, cuyo desarrollo e implementación es responsabilidad del Área Administrativa de la Subdirección Administrativa y Financiera.

Usuarios: El COPNIA es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores del COPNIA (denominados "usuarios") que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología y sistemas de información (TIC).

Los usuarios y custodios de los activos de información del COPNIA son responsables por el uso apropiado, la protección y privacidad de dichos activos.

Activos de información: Teniendo en cuenta que los activos de información son el conjunto de datos que la entidad genera, obtiene, adquiere, transforma o controla, se encuentra prohibido hacer uso de los recursos tecnológicos del COPNIA para almacenar información que no corresponda a los procesos definidos para dar cumplimiento a la misionalidad institucional y por tanto es excluida de cualquier responsabilidad de la entidad.

Toda información que no sea de propósito estrictamente laboral conforme a las funciones del COPNIA y que sea guardada en la infraestructura tecnológica de la Entidad, estará supeditada a su inmediata eliminación, sin previo aviso a sus propietarios.

5.2.2 Clasificación y etiquetado de activos de información

La Entidad debe determinar la clasificación de los activos de información de acuerdo con la criticidad, sensibilidad y reserva de esta. Es responsabilidad del área Administrativa, conforme a lineamientos de gestión documental, liderar y definir las actividades tendientes a identificar y controlar los activos de información de acuerdo con su nivel de confidencialidad y reserva, donde es responsabilidad de cada funcionario validar que los activos se ajusten a la operación de los procesos.

La entidad garantiza la confidencialidad, integridad y disponibilidad de la información, con la aplicación de La Ley 1712 de 2014, también denominada Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional en Colombia, la cual tiene como objetivo fundamental promover la transparencia en la gestión pública y garantizar el derecho de acceso a la información por parte de los ciudadanos; esto representa un paso significativo hacia la consolidación de un gobierno más abierto y participativo, esta legislación establece las bases para la transparencia en la administración pública, reconociendo el derecho fundamental de los ciudadanos a acceder a la información en poder de las entidades gubernamentales.

Por lo anterior, la ley define procedimientos claros y plazos para solicitar información, así como la obligación para las entidades públicas de divulgar de manera proactiva ciertos tipos de información; Este marco normativo busca fortalecer la confianza ciudadana en las instituciones gubernamentales, al tiempo que establece mecanismos para proteger información sensible. Además, la Ley 1712 establece sanciones para aquellos casos en los que las entidades públicas no cumplan con sus disposiciones, garantizando así la efectividad de este instrumento legal en la promoción de una administración pública más abierta, transparente y responsable.

5.2.3 Devolución de activos

La devolución de activos fijos se encuentra enmarcada en el procedimiento de manejo de bienes AB-pr-02. En el momento del retiro de la Entidad, el funcionario se pondrá en contacto con el encargado del área Administrativa, a fin de legalizar la entrega de los bienes que estaban a su cargo. Verificada la información por el encargado de almacén y la conformidad con el inventario, se entrega al funcionario su "Paz y salvo de inventarios".

Todos los funcionarios, contratistas y terceros tienen la responsabilidad de devolver los activos de información que se encuentren a su cargo al terminar su empleo, contrato o vínculo con la Entidad.

Es responsabilidad de la Subdirección Administrativa y Financiera, a través de las áreas de Gestión Humana y Administrativa, definir los procedimientos, formatos y paz y salvos, necesarios para la entrega de activos de información.

Es responsabilidad de los jefes de dependencias y líderes de áreas verificar el cumplimiento de procedimientos y actividades para la entrega y custodia de activos de información, conforme a los equipos de trabajo asignados a cada uno de ellos.

5.2.4 Gestión de medios removibles

Para facilitar el acceso a la información, el COPNIA pone a disposición de sus funcionarios y contratistas autorizados, herramientas tecnológicas de trabajo colaborativo y en la nube, razón por la cual el uso de medios removibles de almacenamiento (cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras) se encuentra restringido y regulado por los

lineamientos de respaldo de activos de información y tablas de retención documental, emitidos por la Subdirección Administrativa y Financiera.

La responsabilidad de la información contenida en los medios removibles es del funcionario que está a cargo del activo, por lo tanto, la información que es almacenada en medios removibles y que debe estar disponible, debe ser protegida para evitar que ésta se vea afectada por el tiempo de vida útil del medio.

5.2.5 Disposición de los activos

Es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones, planificar y dar a conocer las necesidades de recursos necesarios para generación y control de copias de respaldo y almacenamiento de sus activos de información contenidos en los sistemas de información y las bases de datos de la entidad, así como es responsabilidad de la Oficina de Seguridad y Privacidad de la Información de la entidad dar a conocer las necesidades de recursos que se deban aprovisionar para garantizar la disponibilidad, integridad y confidencialidad de la información.

Los puntos y tiempos óptimos de restauración de disponibilidad y recuperación de activos de información son acordados contractualmente con los proveedores, los cuales tienen como umbral de tolerancia 24 horas tanto para RTO (Tiempo óptimo de restauración) como para RPO (Punto Óptimo de restauración). Es responsabilidad de los supervisores de contrato verificar periódicamente el cumplimiento de esta condición.

La Entidad pone a disposición de los funcionarios y contratistas herramientas tecnológicas para el almacenamiento de la información. De acuerdo con lo anterior, todos los activos de información que se generen en herramientas ofimáticas deberán ser guardados en la carpeta de OneDrive configurada en cada uno de los equipos asignados y las versiones de documentos finales deben ser debidamente cargadas y operadas en la plataforma de gestión documental adoptada por la entidad. Es responsabilidad de los funcionarios y contratistas realizar el respectivo backup en esta herramienta y cumplir los parámetros generales de uso descritos con anterioridad (abstenerse de guardar información ajena a la misionalidad institucional), conforme a instrucciones operativas impartidas por el área de Tecnologías de la Información y de las Comunicaciones y a los lineamientos emitidos por la Oficina de Seguridad y privacidad de la información.

5.2.6 Dispositivos móviles y portátiles

No está permitido a los funcionarios del área de Tecnologías de la Información y de las Comunicaciones reparar, desinstalar o instalar software, formatear, dar soporte preventivo o correctivo a equipos personales o que no hagan parte de los activos fijos del COPNIA.

Es responsabilidad del área de Gestión Humana informar la desvinculación o culminación de relación laboral de funcionarios, supernumerarios o planta temporal al área de Tecnologías de la Información y las Comunicaciones. Una vez recibida la comunicación, es responsabilidad del Área de Tecnologías

de la Información y las Comunicaciones retirar todos los accesos a que haya lugar, incluidos dispositivos móviles.

Es responsabilidad de los supervisores informar la desvinculación o culminación de relación laboral de contratistas al área de Tecnologías de la Información y las Comunicaciones. Una vez recibida la comunicación, es responsabilidad del Área de Tecnologías de la Información y las Comunicaciones retirar todos los accesos a que haya lugar, incluidos dispositivos móviles.

En caso de requerir el retiro del dispositivo móvil, es necesario informar al área Administrativa conforme a los procedimientos definidos para tal fin. De presentarse el extravió o hurto de un dispositivo móvil que contenga información de la Entidad, el funcionario será el responsable de reportar de forma inmediata a la Subdirección Administrativa y Financiera y al área de Tecnologías de la Información y las Comunicaciones, quienes identificarán conforme la información contenida, las medidas de seguridad adecuadas para la protección de la información.

Los dispositivos móviles que manejen o administren información confidencial o crítica de la Entidad, no se podrán conectar a una red pública, y deberán ser transportados y usados con extremos cuidados para evitar el daño o manipulación no autorizada de la información, así mismo, será necesario evitar dejar el equipo desatendido o debe ser asegurado con su respectiva guaya.

Se encuentra prohibido realizar instalaciones de aplicaciones que puedan afectar la confidencialidad, integridad y/o disponibilidad de la información almacenada o transmitida por el dispositivo. En todo caso, las instalaciones realizadas en dispositivos móviles deberán realizarse por el área de Tecnologías de la Información y de las Comunicaciones, o con su consentimiento o bajo su supervisión.

Para los dispositivos móviles aplican todos los lineamientos emitidos en el presente manual.

5.2.7 Internet

La oficina de seguridad y privacidad de la información es responsable de la generación de las políticas y área de Tecnologías de la Información y de las Comunicaciones es el responsable de la implementación de lineamientos que permitan la navegación segura y el uso adecuado de este servicio por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

El servicio de internet del COPNIA se encuentra disponible para la ejecución de las labores propias de la función de la entidad; de acuerdo con lo anterior, todos los ingresos establecidos a través de internet pueden ser controlados, monitoreados y reportados por el área de Tecnologías de la Información y de las Comunicaciones, sin previa autorización de los funcionarios o contratistas que tengan el respectivo acceso.

El área de Tecnologías de la Información y de las Comunicaciones se reservan el derecho de filtrado de contenidos que se reciban o envíen desde la red de internet del COPNIA.

Por lo tanto, el filtrado de contenidos se refiere al proceso de controlar o limitar el acceso a ciertos tipos de información, ya sea en línea o en otros medios de comunicación, con el objetivo de prevenir el acceso a contenido no deseado, inapropiado o perjudicial.

Existen diferentes métodos y tecnologías para implementar el filtrado de contenidos, y su aplicación puede variar según el contexto y los objetivos, algunas de sus formas incluyen:

Filtrado de sitios web: Restringir el acceso a sitios web específicos basándose en categorías, palabras clave o direcciones URL. Esto se utiliza para bloquear sitios que pueden contener contenido inapropiado o no deseado.

Filtrado de correos electrónicos: Detectar y bloquear correos electrónicos no deseados o maliciosos mediante el uso de filtros de spam.

Filtrado de contenido en redes sociales: Controlar y limitar el acceso a contenido específico en plataformas de redes sociales para evitar la difusión de información inapropiada o perjudicial.

Filtrado de búsqueda en motores de búsqueda: Modificar los resultados de búsqueda en función de restricciones establecidas para prevenir la visualización de contenido no deseado.

Filtrado en bibliotecas y entornos educativos: Limitar el acceso a ciertos materiales impresos o electrónicos para garantizar que el contenido sea apropiado y cumpla con los estándares establecidos.

Los usuarios del servicio de internet son responsables de evitar prácticas o usos que comprometan la seguridad de la información de la entidad, tales como:

Contraseñas débiles: El uso de contraseñas débiles o fáciles de adivinar puede comprometer la seguridad de las cuentas.

Compartir contraseñas: No se debe compartir información de inicio de sesión o contraseñas con otras personas, ya que esto aumenta el riesgo de acceso no autorizado.

Hacer clic en enlaces sospechosos: Evitar hacer clic en enlaces de correos electrónicos no solicitados o en sitios web sospechosos, ya que podrían contener malware o ser intentos de phishing.

Descargar archivos de fuentes no confiables: La descarga de archivos de sitios web no seguros o el uso de software no autorizado pueden introducir malware en los sistemas, comprometiendo la seguridad de la información.

Uso no autorizado de recursos de red: Evitar el uso indebido de los recursos de red, como ancho de banda excesivo o intentos de intrusión en la red, para mantener la integridad y disponibilidad de los servicios.

Descargas de software no autorizado: no realizar bajo ninguna circunstancia la descarga de copias ilegales de programas comerciales, eludiendo los procesos de licencia y pago, Cracks y

keygens, Software de código abierto sin cumplir con las licencias, Programas maliciosos, copias no autorizadas de freeware.

Se encuentra estrictamente prohibido hacer uso de los servicios tecnológicos del COPNIA para el acceso a páginas relacionadas con pornografía, actividades criminales, terrorismo, crímenes computacionales, y en general todos aquellas páginas y aplicaciones que pongan en riesgo la seguridad y reputación de la entidad.

5.2.8 Correo electrónico, comunicaciones de texto, voz y video

El uso del servicio de correo electrónico está disponible para ingreso desde cualquier sitio con conexión a internet, por esta razón se debe ingresar a este servicio solo desde lugares con acceso a internet conocidos, no se recomienda ingresar a este servicio desde redes públicas.

No se deben usar las cuentas de correo empresariales para envío de correos masivos externos, toda vez que este proceso puede generar el ingreso del dominio copnia.gov.co en listas negras de Spam. De ser necesario enviar correos masivos diarios a usuarios externos que supere más de 1000 cuentas, es necesario comunicarse con el área de Tecnologías de la Información y de las Comunicaciones.

Está prohibido el uso del correo electrónico o de Microsoft Teams (comunicación de texto, voz o video) para el envío, reenvío o intercambio de mensajes no deseados o considerados SPAM (mensajes no solicitados, no deseados o con remitente no conocido), cadenas de mensajes o publicidad.

Se prohíbe el uso de los medios electrónicos de comunicación del COPNIA para el envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

En caso de recibir una comunicación o correo electrónico sospechoso deberá reportarse de inmediato, sin abrirlo, presentando la solicitud de atención del incidente, de acuerdo con lo establecido en el Procedimiento de Atención de Incidencias y requerimientos TIC-pr-01.

El servicio de correo electrónico sólo estará vigente mientras los funcionarios o contratistas tengan relación laboral o contractual con el COPNIA; una vez termine dicha relación, el área de Tecnologías de la Información y de las Comunicaciones eliminará los accesos conforme a comunicación del área de Gestión Humana o de los supervisores de contrato. Se prohíbe hacer uso de los medios electrónicos del COPNIA para el envío de mensajes en donde se divulgue, comente o exprese hechos, opiniones o asuntos internos del COPNIA que puedan afectar la reputación, seguridad e imagen de la entidad.

Se prohíbe a los funcionarios suscribirse con su correo corporativo a listas de correo electrónico, mercadeo, entidades bancarias o grupos de noticias que divulguen información o mensajes ajenos a las funciones y deberes de la entidad.

Los funcionarios y contratistas a quienes se les haya asignado cuentas a medios electrónicos de comunicación de la Entidad serán responsables ante la COPNIA de todos los accesos y actividades que se puedan haber realizado con su usuario y contraseña.

La aplicación Microsoft Teams debe ser utilizada exclusivamente para asuntos laborales, ya que está diseñada para facilitar la comunicación entre usuarios del COPNIA. El uso de video conferencias implica ocupación del ancho de banda de la red y por esta razón se debe utilizar solo para aplicación en asuntos laborales.

5.2.9 Redes Sociales

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador del COPNIA, que sea creado a nombre personal en redes sociales como: X®, Facebook®, YouTube® LinkedIn®, blogs, Instagram, etc., se considera fuera del alcance del Sistema de Gestión de Seguridad de la Información – SGSI del COPNIA, y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

El área de Relacionamiento Interinstitucional y Comunicaciones del COPNIA es responsable de la creación y administración de redes sociales institucionales y su uso está restringido a la difusión de actividades relacionadas con la ejecución estratégica, misional, de apoyo y de evaluación de la Entidad. Los contenidos que se desarrollan se encuentran bajo la supervisión y control de dicha dependencia.

Los funcionarios y contratistas del COPNIA no deben crear cuentas, abrir grupos, o publicar cualquier tipo de información escrita o audiovisual a nombre de la entidad.

5.2.10 Recursos tecnológicos

Todos los equipos de cómputo del COPNIA deben estar enrolados con un usuario estándar de Windows en el dominio del COPNIA, ningún equipo de propiedad del COPNIA debe estar por fuera del dominio, no se permite usuarios de Windows como administradores locales o de dominio, los usuarios administradores solo están configurados para soporte de los equipos y administración de estos.

La infraestructura tecnológica del COPNIA tal como, servidores, equipos activos, PBX y otro tipo de hardware de computador que no resida típicamente en escritorios de usuario o en un área de trabajo común, deben estar ubicados físicamente en un área segura, y se deben implementar los controles

necesarios para la prevención contra riesgos ambientales y no ambientales, que puedan afectar la disponibilidad de los datos.

Es responsabilidad de los funcionarios del COPNIA, hacer uso de los puntos de energía protegidos dispuestos por la entidad, para evitar daños en el hardware de computador.

El área de Tecnologías de la información y de las Comunicaciones debe garantizar que el cableado de telecomunicaciones que transporta los datos o soporta los servicios de información de la Entidad se encuentren adecuadamente protegidos para evitar daño o mala manipulación.

La instalación de cualquier tipo de software en los equipos de cómputo del COPNIA, es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones, y por tanto son los únicos autorizados para realizar o autorizar esta labor.

Es responsabilidad del área Administrativa presupuestar y programar los mantenimientos preventivos y correctivos para los equipos, de acuerdo con las especificaciones e intervalos de servicio recomendados por los fabricantes. El área de Tecnologías de la Información y de las Comunicaciones deberá mantener los registros de las fallas reportadas por los usuarios.

Se deben asegurar los equipos fuera de las instalaciones de la organización y su salida debe estar autorizada conforme a procedimientos establecidos para tal fin.

Toda la información del COPNIA tendrá que ser removida del equipo antes de su disposición o reutilización.

Antes de cualquier venta o donación, todos los medios de almacenamiento deben ser borrados de acuerdo con los mecanismos de eliminación de información que adopte la entidad.

Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla definido por la Entidad. Estos cambios pueden ser realizados únicamente por el área de Tecnologías de la Información y de las Comunicaciones; para ello se debe disponer de un estándar de seguridad para estaciones de trabajo independientemente del sistema operativo.

El área de Tecnologías de la Información y de las Comunicaciones define e informa la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realiza el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

El área de Tecnologías de la Información y de las Comunicaciones no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean del COPNIA.

5.2.11 Escritorio y pantalla despejada

Los funcionarios, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con el COPNIA deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Los usuarios de los sistemas de información y comunicaciones del COPNIA deben bloquear la pantalla de su computador con el protector de pantalla, cuando no se esté utilizando el equipo o cuando por cualquier motivo, deba dejar su puesto de trabajo.

Por política de seguridad de información en el dominio COPNIA, se bloqueará automáticamente la pantalla después de 15 minutos de inactividad de la misma.

Los usuarios de los sistemas de información y comunicaciones del COPNIA deben cerrar las aplicaciones y servicios de red cuando ya no los necesiten.

Al imprimir documentos con información pública reservada y/o pública clasificada (semiprivada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

No se debe utilizar fotocopiadoras, escáneres, periféricos, cámaras digitales y en general equipos tecnológicos que no se encuentren administrados por el dominio COPNIA.

5.2.12 Gestión de Hardware

Cualquier cambio que se requiera realizar en los equipos de cómputo de la Entidad (cambios de procesador, monitor, teclado, mouse, adición de memoria o tarjetas) debe tener previamente una evaluación y autorización técnica del área de Tecnologías de la Información y de las Comunicaciones.

La reparación técnica de los equipos, que implique la apertura de estos, únicamente puede ser realizada por personal capacitado, previa autorización del supervisor del contrato de mantenimiento y del responsable del manejo de bienes.

Los equipos de cómputo (PC, servidores, comunicaciones, etc.) no deben moverse o reubicarse sin previa autorización de los responsables del manejo de bienes.

Todo funcionario está obligado a atender los lineamientos establecidos en el Procedimiento de manejo de bienes adoptado por la entidad, referente a cualquier movimiento o modificación que se lleve a cabo con los equipos asignados.

El funcionario designado para supervisar los contratos de mantenimiento será el encargado de diseñar y ejecutar planes de mantenimiento preventivo a los equipos del COPNIA.

5.2.13 Gestión de Software

Los líderes funcionales del COPNIA son quienes determinan e informan al Área de Tecnologías de la Información y las Comunicaciones los permisos que cada uno de los funcionarios deben tener sobre las aplicaciones COPNIA, tomando como guía las tablas de control de acceso adoptadas por la entidad.

Los líderes funcionales son los únicos que pueden avalar cambios sobre los aplicativos, como actualizaciones, modificaciones, desarrollos, respaldos o dar de baja algún sistema de información.

Los líderes funcionales podrán requerir en cualquier momento al área de tecnologías de la Información y de las Comunicaciones una matriz de roles y perfiles con los usuarios activos a la fecha, para que se determine si se requiere hacer algún cambio que debe ser oficializado según el procedimiento de Atención de Incidencias y Requerimientos, TIC-pr-01.

Cada funcionario es responsable del buen uso de su usuario dentro de los aplicativos del COPNIA, teniendo en cuenta que son ambientes productivos, por lo tanto, no debe ingresar información inválida, incorrecta, ficticia o de prueba.

Está prohibido realizar actualizaciones, modificaciones, inserciones o eliminaciones directamente en las bases de datos del COPNIA, omitiendo la capa de aplicación y los registros de auditoria propios de los sistemas de información, estas actualizaciones en casos especiales deben realizarse debidamente controladas y documentadas en el proceso TIC-PR-01 con la autorización de los lideres funcionales.

Las actualizaciones del ecosistema tecnológico de la entidad se deben manejar acorde al ANEXO 1- PROGRAMACIÓN DE ACTUALIZACIONES PARA COPNIA SOBRE LA PLATAFORMA TECNOLÓGICA

La administración de las bases de datos del COPNIA es realizada únicamente por el área de Tecnologías de la Información y de las Comunicaciones, quienes en ninguna circunstancia pueden alterar la información allí contenida. Se podrán realizar actividades de soportes sobre la base de datos en caso de algún error de las aplicaciones o de alguna imposibilidad técnica, que debe estar reportado y documentado según el procedimiento de Atención de Incidencias y Requerimientos, TIC-pr-01.

No se pueden generar copias de las bases de datos sin una autorización escrita del profesional de gestión del área de Tecnologías de la Información y de las Comunicaciones, ni se deben entregar copias o accesos a terceros o proveedores sin la misma autorización.

Los cambios de software se realizarán siempre en un ambiente de pruebas dispuesto por la entidad; estos cambios deben ser avalados por escrito por el líder funcional del sistema de información o plataforma, quien autorizará el paso a producción.

Una vez sea superada la etapa de pruebas, el área de Tecnologías de la Información y de las Comunicaciones documenta y coordina el paso a producción.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros deberá realizarse sin la alteración de la seguridad y acorde al procedimiento TIC-PR-02 Controles de cambio.

El área de Tecnologías de la Información y de las Comunicaciones deberá verificar que los cambios sean propuestos por usuarios autorizados y se encuentren alineados a la licencia de uso y necesidades de la entidad.

El área de Tecnologías de la Información y de las Comunicaciones garantizará que la implementación de los cambios se lleve a cabo sin generar interrupción de las actividades operativas, de no ser posible por las actividades propias de los cambios, se debe programar una ventana de mantenimiento para informar de la hora de inicio y hora de finalización donde se encontrará indisponibilidad parcial o completa de los servicios.

Los responsables de los cambios deberán informar antes de la implementación de un cambio a las áreas o usuarios que puedan verse afectados, con el fin de evitar la alteración de los procesos y la operatividad de la entidad para el cumplimiento de la misión institucional.

5.2.14 Política de Implementación de BitLocker para la Encripción de Equipos de Cómputo para Usuarios Finales

1. Propósito y Alcance

Esta política tiene como objetivo establecer directrices y procedimientos para la implementación de BitLocker en los equipos de cómputo utilizados por los usuarios finales de la entidad. La encripción de dispositivos con BitLocker es esencial para proteger la confidencialidad y la integridad de los datos almacenados en dichos equipos.

2. Definiciones

a. BitLocker: BitLocker es una tecnología de encripción de disco completo integrada en los sistemas operativos Windows que protege los datos almacenados en los dispositivos de cómputo mediante la encripción de todo el disco.

3. Implementación de BitLocker

a. Requisitos Mínimos: Todos los equipos de cómputo utilizados por usuarios finales que contengan información confidencial o sensible deben tener BitLocker habilitado y configurado.

b. Configuración de BitLocker: BitLocker debe configurarse con una autenticación sólida, como un PIN o una clave de recuperación. Los dispositivos de cómputo deben estar actualizados con las últimas políticas de seguridad de BitLocker.

c. Clave de Recuperación: Se deben generar y almacenar claves de recuperación de BitLocker de manera segura. Estas claves son esenciales para el desbloqueo en caso de olvido del PIN u otras situaciones de emergencia.

d. Procedimiento de desbloqueo: Se proporcionarán procedimientos y recursos a los usuarios finales para desbloquear sus dispositivos en caso de olvido del PIN o problemas de inicio de sesión a través de ticket de servicio.

4. Revisiones y Monitoreo

a. La Oficina de Seguridad y Privacidad de la Información, llevará a cabo revisiones regulares para verificar el cumplimiento de la encripción de dispositivos con BitLocker.

5. Excepciones

a. En situaciones excepcionales donde la implementación de BitLocker no sea técnicamente posible o razonable, se requerirá la aprobación de la Oficina de Seguridad y Privacidad de la Información y se deberán tomar medidas de seguridad alternativas.

6. Capacitación y Concienciación

a. La entidad proporcionará capacitación y concienciación a los usuarios finales sobre la importancia de la encripción de dispositivos con BitLocker y la correcta gestión de las claves de recuperación.

7. Cumplimiento y Sanciones

a. El incumplimiento de esta política podría dar lugar a medidas disciplinarias, de acuerdo con las políticas de seguridad de la entidad.

8. Revisiones de Política

a. Esta política será revisada anualmente o según sea necesario para garantizar su eficacia y relevancia.

La implementación de BitLocker en los equipos de cómputo para usuarios finales es esencial para garantizar la seguridad de los datos y la protección de la información confidencial. Cumplir con esta política es fundamental para mantener un ambiente de cómputo seguro y confiable en toda la entidad.

5.2.15Backups o Copias de respaldo

Teniendo en cuenta que el COPNIA dispone de medios de almacenamiento en la nube, los funcionarios y contratistas de la entidad son los responsables de la información que reposa en sus equipos de cómputo y de su debido respaldo.

Es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones brindar soporte a los funcionarios y contratistas con el fin de garantizar el respaldo adecuado de la información que se encuentra alojada en las estaciones de trabajo y es responsabilidad de validación del adecuado respaldo de la información por parte de la oficina de seguridad y privacidad de la información.

Por lo tanto, con las novedades de retiro se debe proceder de la siguiente forma:

Novedad de retiro dentro del procedimiento TIC-PR01:

Cuando se notifique el retiro de un usuario a través del procedimiento TIC-PR-01, el área de gestión humana informa al área de tecnología para iniciar el proceso de descarga e inactivación de la cuenta de office 365.

Descarga de la Cuenta de Office 365:

El área de tecnología será responsable de realizar la copia de los datos existentes en la cuenta de Office 365 del usuario que se retira.

Transferencia a OneDrive:

Una vez que se haya completado la descarga de los datos, el área de tecnología transferirá los archivos a la cuenta de OneDrive designada específicamente para este propósito.

Se generará un link compartido y se enviará al jefe inmediato del usuario que se retira para su revisión y, si es necesario, para transferir la responsabilidad de los archivos a otros usuarios.

Depuración Semestral:

Se llevará a cabo una depuración semestral de los datos almacenados en la cuenta de OneDrive designada, esto para liberar espacio de almacenamiento, dado que el jefe inmediato en este periodo prudencial ya debe tener designada la responsabilidad de la información en otras cuentas de usuario.
Los jefes inmediatos son responsables de revisar los datos transferidos y notificar al área de tecnología sobre cualquier problema o acción necesaria.

5.2.16 Política de Objetivos de Punto de Recuperación (RPO) y Objetivos de Tiempo de Recuperación (RTO) de 24 Horas para los sistemas de información

1. Propósito y Alcance

Esta política tiene como objetivo establecer los Objetivos de Punto de Recuperación (RPO) y los Objetivos de Tiempo de Recuperación (RTO) para los sistemas de información de la entidad con el fin de garantizar la disponibilidad y continuidad de los sistemas de información críticos en un plazo

máximo de 24 horas. Esta política se aplica a todos los sistemas, aplicaciones y datos considerados esenciales para las operaciones de la entidad, aplicado por el área de Tecnologías de la Información y de las Comunicaciones de la entidad.

2. Objetivos de Punto de Recuperación (RPO)

a. Definición de RPO: El RPO se define como el periodo de tiempo máximo durante el cual la entidad está dispuesta a tolerar la pérdida de datos antes de que impacte significativamente en sus operaciones.

b. RPO de 24 Horas: La entidad establece un RPO de 24 horas, lo que significa que no se permite una pérdida de datos significativa que exceda dicho periodo. Todos los sistemas y aplicaciones críticas deben estar respaldados y protegidos para cumplir con este objetivo.

c. Procedimientos de Respaldo: La entidad implementará procedimientos de respaldo regulares y automatizados para garantizar que se cumpla con el RPO de 24 horas. Todos los datos críticos deben ser respaldados de manera consistente y segura.

3. Objetivos de Tiempo de Recuperación (RTO)

a. Definición de RTO: El RTO se define como el tiempo máximo permitido para la recuperación de sistemas y aplicaciones críticas después de una interrupción o desastre.

b. RTO de 24 Horas: La entidad establece un RTO de 24 horas, lo que significa que todos los sistemas y aplicaciones críticas deben ser restaurados y estar completamente operativos dentro de dicho plazo.

c. Procedimientos de Recuperación: La entidad implementará procedimientos de recuperación de desastres y planes de continuidad de negocio que permitan cumplir con el RTO de 24 horas. Estos procedimientos deben ser revisados y probados regularmente.

4. Responsabilidades

a. Responsabilidades de la Alta Dirección: La alta dirección de la entidad es responsable de asignar los recursos necesarios para cumplir con los objetivos de RPO y RTO de 24 horas.

b. Responsabilidades del Área de Tecnologías de la Información y de las Comunicaciones, TIC: El Área TIC es responsable de implementar, monitorear y mantener los procedimientos de respaldo y recuperación necesarios para cumplir con los objetivos de RPO y RTO.

5. Pruebas y Ejercicios

a. La entidad, a través del área TIC, llevará a cabo pruebas y ejercicios regulares para evaluar la capacidad de recuperación de sistemas y aplicaciones críticas y garantizar que se cumplan los RPO y RTO de 24 horas.

b. La entidad a través del área TIC adelantará las pruebas periódicas de integridad de backups según lo descrito en el documento ANEXO 2-PROGRAMACION DE REVISION DE BACKUPS PARA COPNIA SOBRE LA PLATAFORMA TECNOLOGICA

6. Cumplimiento y Revisión

a. La Oficina de Seguridad y Privacidad de la Información se asegurará de que se realicen revisiones periódicas para verificar el cumplimiento de esta política y la efectividad de los procedimientos de respaldo y recuperación.

Cumplir con los Objetivos de Punto de Recuperación (RPO) y Objetivos de Tiempo de Recuperación (RTO) de 24 horas es esencial para garantizar la continuidad de las operaciones y la disponibilidad de los sistemas críticos de la entidad. Esta política es un componente clave en el marco de seguridad de la información para mitigar riesgos y mantener la resiliencia operativa.

5.3 Control de Acceso[3]

5.3.1 Control de accesos con usuarios y contraseñas

El área de Tecnologías de la Información y de las Comunicaciones es responsable de que todos los usuarios sean identificados independientemente, con permisos de acceso específicos e individuales para el acceso a redes, aplicaciones, y sistemas de información del COPNIA, autorizados por razones básicas de sus funciones, por el área de Gestión Humano.

El área de Tecnologías de la Información y de las Comunicaciones suministrará a los usuarios autorizados por el área de Gestión Humano contraseñas o claves para el acceso a los servicios de red, sistemas de información y/o servicios TIC. Es responsabilidad de los usuarios cambiar la contraseña inicial, conforme a los parámetros definidos para cada servicio tecnológico y encargarse de su respectiva administración.

El área de Tecnologías de la Información y de las Comunicaciones suministrará una matriz de roles y perfiles para la gestión de permisos definidos por los líderes funcionales, la cual debe estar alineada a las tablas de control de acceso adoptadas por la entidad.

Los líderes de área o funcionales determinan los permisos adicionales requeridos para la ejecución de labores y gestionan con el área de Tecnologías de la Información y de las Comunicaciones

[3] Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales la Entidad determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos.

novedades como la modificación, activación o inactivación de usuarios, siguiendo el procedimiento de Atención de Incidencias y Requerimientos, TIC-pr-01.

Los usuarios y contraseñas asignados a funcionarios, contratistas o terceros que tengan permisos de acceso a redes, aplicaciones y sistemas de información del COPNIA, son de uso personal e intransferible, por lo cual no se permite compartirlos o prestarlos.

Ningún usuario deberá acceder a la red, sistemas de información o a los servicios TIC del COPNIA utilizando una cuenta de usuario o clave diferente a la asignada.

Para facilitar el acceso a las aplicaciones disponibles, mediante el uso de un número reducido de claves y contraseñas por usuario, el área de Tecnologías de la Información y de las Comunicaciones se encargará de que dichos accesos se realicen con vinculación directa de las credenciales de los usuarios de directorio activo.

Las conexiones a servicios en la nube dispuestos por la entidad, tales como Office 365, deben realizarse desde sitios seguros, evitando conexiones en lugares tales como café internet, equipos móviles desconocidos o sitios de bajo nivel de confianza, entre otros.

Es responsabilidad de los funcionarios y contratistas del COPNIA realizar el cierre de sesiones por cada caso de ingreso a cualquiera de las aplicaciones o servicios tecnológicos que requieran acceso mediante usuarios y contraseña. La práctica de cierres de ventanas conlleva el riesgo de permitir el ingreso a los sitios del COPNIA a personas no autorizadas.

El Área de Tecnologías de la Información y de las Comunicaciones es responsable de fomentar y programar desconexiones por tiempo sin uso temporal de aplicaciones y computadores personales activos.

5.3.2 Política de Revisión y Mantenimiento de Matriz de Roles y Perfiles

1. Propósito y Alcance

Esta política tiene como objetivo establecer un proceso para la revisión y mantenimiento mensual de la matriz de roles y perfiles de acceso a los sistemas de información en la entidad. Se aplica a todos los líderes funcionales de cada sistema de información y al personal del área de Tecnologías de la Información y Comunicación (TIC) encargado de coordinar este proceso.

2. Definiciones

a. Matriz de Roles y Perfiles: Documento que describe los roles y perfiles de acceso a los sistemas de información, especificando las responsabilidades y los niveles de acceso de los usuarios.

b. Líder Funcional: Responsable designado para cada sistema de información, encargado de la revisión y mantenimiento de la matriz de roles y perfiles.

3. Responsabilidades

a. Área de Tecnologías de la Información y las Comunicaciones - TIC:

i. El área TIC será responsable de enviar mensualmente a los líderes funcionales de cada sistema de información la matriz de roles y perfiles correspondiente.

ii. El área TIC brindará asistencia y orientación a los líderes funcionales en el proceso de revisión y mantenimiento de la matriz de roles y perfiles.

b. Líderes Funcionales:

i. Los líderes funcionales deben revisar la matriz de roles y perfiles de su sistema de información mensualmente.

ii. Si un líder funcional considera que es necesario realizar alguna eliminación, modificación o adición en la matriz de roles y perfiles, deberá completar una solicitud por ticket de servicio y enviarla al área TIC para su revisión y procesamiento.

iii. Los líderes funcionales deben garantizar que las modificaciones propuestas cumplan con las políticas de seguridad y los principios de menor privilegio.

El principio del menor privilegio es un concepto fundamental en seguridad informática que sostiene que un usuario, programa o sistema debería tener solo los privilegios necesarios para realizar sus funciones específicas y no más. por lo tanto, se busca limitar el acceso y los permisos a lo esencial para evitar posibles riesgos y daños en caso de una eventual vulneración de seguridad. Al adherirse a este principio, se reduce la superficie de ataque, ya que se minimizan las oportunidades para que usuarios malintencionados o malware exploren y exploten posibles debilidades. Este enfoque de seguridad contribuye a mitigar riesgos al restringir el acceso a recursos y funciones solo a aquellos que son esenciales para las tareas particulares de un usuario o sistema, fortaleciendo así la resiliencia y protección en entornos digitales.

4. Proceso de Revisión y Mantenimiento

a. Los líderes funcionales deben llevar a cabo una revisión mensual de la matriz de roles y perfiles, verificando que los niveles de acceso y las responsabilidades se ajusten a las necesidades operativas y de seguridad.

b. Cualquier cambio propuesto en la matriz de roles y perfiles debe ser documentado en el ticket de servicio, especificando la razón de la modificación y los detalles de la misma.

c. El área TIC revisará las solicitudes de modificación de roles y perfiles, asegurando que cumplen con las políticas de seguridad y los procedimientos establecidos.

d. Una vez aprobada la solicitud de modificación, el área TIC actualizará la matriz de roles y perfiles y notificará al líder funcional sobre la implementación de los cambios.

5. Cumplimiento y revisiones

a. La Oficina de Seguridad y Privacidad de la Información llevará a cabo revisiones regulares para verificar el cumplimiento de esta política y el correcto proceso de revisión y mantenimiento de la matriz de roles y perfiles.

6. Capacitación y Concienciación

a. La entidad proporcionará capacitación y concienciación regular a los líderes funcionales y al personal del área TIC sobre la importancia de la revisión y el mantenimiento de la matriz de roles y perfiles.

7. Revisiones de Política

a. Esta política será revisada anualmente o según sea necesario para garantizar su eficacia y relevancia.

La revisión y el mantenimiento de la matriz de roles y perfiles son esenciales para garantizar que los accesos a los sistemas de información sean adecuados y seguros. Cumplir con esta política es fundamental para mantener un ambiente de seguridad de la información confiable y alineado con las necesidades operativas de la entidad.

5.3.3 Política de Autenticación de Doble Factor (MFA) a través de Correo Electrónico, Mensaje de Texto o aplicaciones al Celular

1. Propósito y Alcance

Esta política tiene como objetivo establecer directrices claras y medidas de seguridad relacionadas con la autenticación de doble factor (MFA) en el acceso a sistemas, aplicaciones y datos a través de correo electrónico y mensajes de texto o aplicaciones al celular. Esta política se aplica a todos los usuarios y sistemas dentro de la entidad y busca garantizar un nivel adecuado de seguridad en el acceso a la información crítica.

2. Definiciones

a. Autenticación de Doble Factor (MFA): Método de autenticación que requiere la presentación de al menos dos formas diferentes de identificación antes de permitir el acceso a los sistemas o datos.

3. Implementación de MFA

a. Requerimiento de MFA: La entidad implementará la autenticación de doble factor (MFA) para todos los sistemas y aplicaciones que contengan información crítica o sensible, de acuerdo con las funcionalidades disponibles en las plataformas tecnológicas utilizadas.

b. Medios de Autenticación: La entidad utilizará correo electrónico y/o mensajes de texto al celular como medios de autenticación de doble factor. Los usuarios deberán registrarse y mantener sus datos de contacto actualizados.

c. Registro y Configuración: Los usuarios serán responsables de registrar y configurar su método de autenticación MFA siguiendo las instrucciones proporcionadas por la oficina de seguridad y privacidad de la información. Los usuarios deberán configurar sus dispositivos móviles y direcciones de correo electrónico de manera segura.

d. Códigos de Respaldo: Se proporcionarán códigos de respaldo para cada usuario registrado en MFA. Estos códigos deberán mantenerse en un lugar seguro y no compartirse con otras personas. Los usuarios serán responsables de regenerar los códigos de respaldo en caso de pérdida o compromiso.

4. Excepciones

a. En situaciones excepcionales, donde la implementación de MFA no sea técnicamente posible o viable, se deben documentar las razones y se requerirá la aprobación por la Oficina de Seguridad y Privacidad de la Información.

5. Cumplimiento y Revisiones

a. La Oficina de Seguridad y Privacidad de la Información será responsable de revisar el cumplimiento de esta política de forma regular. Los usuarios que no cumplan con las directrices establecidas podrán enfrentar medidas disciplinarias.

6. Capacitación y Concienciación

a. La entidad proporcionará capacitación y concienciación continua a los usuarios sobre la importancia de la MFA y la correcta configuración de sus métodos de autenticación.

7. Revisiones de Política

a. Esta política será revisada anualmente o según sea necesario para garantizar su relevancia y efectividad.

Esta política de autenticación de doble factor (MFA) tiene como objetivo fortalecer la seguridad de la entidad y garantizar la protección de la información crítica. El cumplimiento de esta política es esencial para mantener un ambiente seguro y confiable para todos los usuarios y sistemas.

5.3.4 Suministro del control de acceso

Contraseñas de infraestructura tecnológica

Es responsabilidad del líder del área de Tecnologías de la Información y de las Comunicaciones suministrar, conservar y custodiar las claves de acceso otorgadas a funcionarios con usuarios con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad. Los usuarios con privilegios superiores y sus correspondientes contraseñas a consolas administrables, accesos a sistemas de información, servidores o infraestructura, se dejan en custodia al líder de Tecnologías de la Información y de las Comunicaciones, quien asignará accesos a los funcionarios del área, según funciones y niveles de responsabilidad.

El personal del área de Tecnologías de la Información y de las Comunicaciones debe emplear de manera obligatoria las claves o contraseñas con el más alto nivel de complejidad disponible para cada aplicación, sistema de información o infraestructura, utilizando los servicios de autenticación fuerte disponibles para cada uno de ellos.

Los administradores de los sistemas de información deben seguir los lineamientos de gestión de contraseñas definidas en este documento y notificar cualquier cambio al líder del área de Tecnologías de la Información y de las Comunicaciones, quien se encargará de la custodia centralizada de las claves o contraseñas, en un sitio seguro.

Es responsabilidad de los funcionarios que cuenten con usuarios con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información mantener informado al líder del área de Tecnologías de la Información y de las Comunicaciones, de cualquier cambio ocurrido en los usuarios y claves de acceso otorgados para la labor encomendada.

Es responsabilidad de los funcionarios del área de Tecnologías de la Información y de las Comunicaciones asegurarse que de que las contraseñas referentes a las cuentas "predefinidas o por default" incluidas en los sistemas, hardware o aplicaciones adquiridas que se encuentre bajo su responsabilidad sean desactivadas. De no ser posible su desactivación, las contraseñas serán cambiadas después de la instalación del producto. Las anteriores actividades deben ser informadas al líder del área de Tecnologías de la Información y las Comunicaciones.

Los usuarios y claves de los administradores de sistemas y del personal del área de Tecnologías de la Información y de las Comunicaciones son de uso personal e intransferible, por lo tanto, los funcionarios del área en mención no deben dar a conocer sus claves a terceros. En caso de ser requerido algún acceso o soporte que exija dar a conocer dicha información, se debe solicitar autorización del profesional de gestión del área, quien documentará e impartirá instrucciones especiales al respecto.

La oficina de seguridad y privacidad de la información en el COPNIA desempeña un papel central al establecer las reglas y directrices necesarias para garantizar un acceso controlado, ya sea físico o lógico, a la información y plataformas informáticas cruciales para la entidad. Esta oficina se dedica

a diseñar políticas que abordan tanto la seguridad física de los entornos donde se almacena y procesa la información como la gestión de accesos lógicos a través de sistemas y redes. Estas reglas buscan no solo proteger la confidencialidad y la integridad de los datos, sino también garantizar que solo aquellos usuarios autorizados tengan la capacidad de interactuar con las plataformas informáticas del COPNIA. Al establecer un marco sólido de control de acceso, la Oficina de Seguridad y Privacidad de la Información contribuye a salvaguardar la información sensible y a fortalecer la postura general de seguridad cibernética de la organización.

El Área de Tecnologías de la Información y las Comunicaciones implementa las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática del COPNIA.

La conexión remota a la red de área local del COPNIA debe realizarse a través de una conexión VPN segura (Red privada virtual) suministrada por la entidad, la cual debe ser aprobada, registrada y monitoreada por el Área de Tecnologías de la Información y de las Comunicaciones. El uso de esta herramienta está establecido solo para uso laboral. No se debe suministrar configuración de usuarios o datos de conexión a personas ajenas del COPNIA ni se debe configurar la VPN en equipos ajenos a la entidad.

5.3.5 Política de Asignación y Uso de Derechos de Acceso Privilegiado

1. Propósito y Alcance

Esta política tiene como objetivo establecer directrices para la asignación y el uso de derechos de acceso privilegiado dentro de la entidad con el fin de garantizar la seguridad, la integridad y la confidencialidad de la información y los sistemas críticos. Esta política se aplica a todos los usuarios y administradores de sistemas que requieran derechos de acceso privilegiado.

2. Definiciones

a. Derechos de Acceso Privilegiado: Se refiere a la autorización y los permisos otorgados a usuarios o administradores de sistemas para acceder a recursos críticos, realizar tareas de administración y modificar configuraciones sensibles.

3. Asignación de Derechos de Acceso Privilegiado

a. Justificación: Los derechos de acceso privilegiado solo se asignarán después de una justificación válida y documentada que demuestre la necesidad de dichos derechos para el desempeño de tareas específicas, mediante solicitud del administrador del sistema por medio de ticket de servicio al área TIC.

b. Identificación de Usuarios: Los usuarios que requieran derechos de acceso privilegiado serán identificados y autenticados de manera segura antes de recibir tales privilegios, siendo evaluada la factibilidad por parte del profesional de gestión del área TIC y el profesional de

gestión de la Oficina de Seguridad y Privacidad de la Información, aval que será manifestado por correo electrónico.

c. Principio de Menor Privilegio: Los derechos de acceso privilegiado se asignarán siguiendo el principio de menor privilegio, lo que significa que los usuarios solo tendrán acceso a los recursos y las funciones necesarios para llevar a cabo sus tareas específicas.

d. Revisión Periódica: La asignación de derechos de acceso privilegiado se revisará de forma regular y se ajustará según sea necesario. Los derechos que ya no sean necesarios se revocarán de inmediato.

4. Uso de Derechos de Acceso Privilegiado

a. Responsabilidad: Los usuarios con derechos de acceso privilegiado deben utilizar estos privilegios de manera responsable y solo para las tareas autorizadas. No se permitirá el uso de estos privilegios para fines personales o no autorizados.

b. Registro de Actividades: Se llevará un registro de todas las actividades realizadas con derechos de acceso privilegiado. Los registros deben ser revisados y supervisados de forma regular por parte del área TIC.

c. Mantenimiento de Contraseñas: Las contraseñas de cuentas con derechos de acceso privilegiado deben cumplir con los estándares de seguridad y ser actualizadas de manera regular.

5. Cumplimiento y revisiones

La Oficina de Seguridad y Privacidad de la Información realizará revisiones regulares para verificar el cumplimiento de esta política y la correcta asignación y uso de derechos de acceso privilegiado.

6. Capacitación y Concienciación

a. La entidad proporcionará capacitación y concienciación regular a los usuarios con derechos de acceso privilegiado sobre las responsabilidades y prácticas seguras.

7. Cumplimiento y Sanciones

a. El incumplimiento de esta política podría dar lugar a medidas disciplinarias, de acuerdo con las políticas de seguridad de la entidad.

8. Revisiones de Política

a. Esta política será revisada anualmente o según sea necesario para garantizar su eficacia y relevancia.

La asignación y el uso de derechos de acceso privilegiado son fundamentales para garantizar la seguridad y la integridad de la información y los sistemas de la entidad. Cumplir con esta política es esencial para mitigar riesgos y mantener un entorno de seguridad de la información confiable.

5.3.6 Contraseñas de plataformas tecnológicas administradas por terceros

Cuando la entidad requiere que la administración de una plataforma tecnológica sea desarrollada por un tercero, se deben seguir los siguientes lineamientos para el manejo de cuentas y contraseñas:

1. Una vez establecida la relación contractual del COPNIA con su respectivo proveedor de servicios administrados de plataforma tecnológicas, cada proveedor debe solicitar por escrito al supervisor del contrato la asignación de una cuenta de usuario y contraseña, definiendo claramente el alcance y actividades a realizar con la misma.

2. El supervisor del contrato solicita por medio de un ticket de servicio al área de Tecnologías de la Información y de las Comunicaciones de COPNIA la asignación de una cuenta de usuario y contraseña de manejo exclusivo del contratista (Procedimiento de Atención de Incidencias y Requerimientos TIC-pr-01). El supervisor de contrato especificará la cuenta de correo electrónico a la cual se debe realizar la entrega de las credenciales, donde por parte del área de Tecnologías de la Información y de las Comunicaciones se validará si procede o no el requerimiento elevado.

3. El área de Tecnologías de la Información y de las Comunicaciones del COPNIA emite una cuenta de usuario y contraseña de manejo exclusivo del contratista, donde aplicará los principios de contraseñas seguras, y realizará la respectiva entrega directamente a la cuenta de correo suministrada por el supervisor del contrato al contratista.

4. Una vez se realiza la entrega de estas credenciales al contratista, este será el único responsable de las acciones allí derivadas, donde debe acogerse a las políticas del presente Manual de Seguridad de la Información y salvaguardar los principios de confidencialidad, seguridad y disponibilidad de la información, así como el cumplimiento de las obligaciones generales y específicas de seguridad y confidencialidad del contrato. Esto conlleva a que toda acción que vaya a realizar el contratista debe contar con la debida autorización por escrito del supervisor del contrato.

5. Una vez terminada la relación contractual entre el contratista y la Entidad, el contratista por escrito realizará el retorno de las credenciales, para que el supervisor del contrato solicite mediante ticket de servicio al área TIC su respectiva desactivación.

5.3.7 Gestión de contraseñas

La solicitud del restablecimiento de contraseñas solo puede ser realizado por el usuario titular de la cuenta o de su jefe inmediato, mediante requerimiento escrito, conforme a las directrices del procedimiento de Atención de Incidencias y Requerimientos TIC-pr-01. Es responsabilidad del funcionario del área de Tecnologías de la Información y de las Comunicaciones asignado para la labor, verificar el estricto cumplimiento del procedimiento, así como validar la identidad y competencia del solicitante, antes de proceder.

Es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones configurar las contraseñas de los servicios de Directorio Activo y Correo, de tal forma que cumplan las siguientes reglas o condiciones:

- Las contraseñas deben tener mínimo ocho (8) caracteres alfanuméricos, de los cuales, por lo menos uno debe ser una letra en mayúscula, uno (1) en minúscula y uno (1) numérico. Ej. Sinfonica07.

- Las contraseñas deben tener una vigencia de máximo 40 días. Transcurrido el periodo, los servicios deben requerir el cambio.

- Cada vez que se requiera un cambio, ya sea por requerimiento del usuario o expiración de las contraseñas, los servicios deberán validar que las nuevas contraseñas sean diferentes a las últimas cinco que hayan sido usadas por la cuenta.

- Los servicios deberán parametrizarse para que las contraseñas se bloqueen después de 3 intentos erróneos. En caso de que la situación descrita se presente, el desbloqueo de claves se realizará siguiendo el procedimiento de Atención de Incidencias y Requerimientos, TIC-pr-01.

Se recomienda a los usuarios abstenerse de asignar contraseñas que contengan información personal tal como nombres propios, de familiares o de mascotas, apellidos y fechas de cumpleaños, entre otros, ya que estas prácticas pueden ser detectadas y usadas en contra de la seguridad de la información de la entidad.

5.3.8 Perímetro de seguridad

Las áreas dispuestas por la Entidad para la atención al público son las ventanillas de correspondencia de cada oficina, por lo cual no es permitido el acceso de visitantes a las oficinas de las diferentes áreas de la Entidad, a excepción de contratistas. En caso de que se requiera el acceso de personal diferente, este deberá ser autorizado por el profesional de gestión del área Administrativa o por el secretario regional o seccional, en los casos correspondientes; para esto, el funcionario que estará a cargo del visitante deberá solicitar autorización para el ingreso de este mediante correo electrónico a los funcionarios mencionados anteriormente según sea el caso.

Todo ingreso de funcionarios y personal externo en horario no hábil deberá ser autorizada previamente por el profesional de gestión del área Administrativa o el secretario regional o seccional cuando corresponda, para lo cual, debe remitirse un correo electrónico por el funcionario o por el jefe del área quien deberá ser informado al respecto.

Las puertas de acceso a las oficinas deberán permanecer cerradas durante la jornada laboral y debidamente aseguradas en horario no laboral, es responsabilidad de todos los funcionarios garantizar el cierre de estas a su salida. Con el fin de salvaguardar los equipos de la Entidad estos deben estar asegurados en la medida de lo posible privilegiando el uso de guaya.

Al finalizar la jornada laboral deben quedar las ventanas de cada oficina cerradas y tanto las luces como los equipos apagados. Es responsabilidad de cada funcionario velar por estas condiciones, haciendo uso razonable de los recursos de la Entidad.

Todos los funcionarios deberán portar su carné en un lugar visible mientras permanezcan dentro de las instalaciones del COPNIA.

Política de acceso a las instalaciones o depósitos de archivo:

Autorización e Identificación:

Objetivo: Garantizar que el acceso a las instalaciones o depósitos de archivo esté limitado a personal autorizado.

Procedimientos:

- Solo el personal designado y autorizado tiene permiso para acceder, designado por el profesional de gestión del área administrativa.
- La identificación y autenticación son obligatorias para todas las personas autorizadas.

Seguridad Física:

Objetivo: Proteger las instalaciones y los documentos almacenados contra accesos no autorizados y posibles riesgos físicos.

Procedimientos:

- Implementación de sistemas de control de acceso, como cerraduras electrónicas o biométricas.
- Implementar alarmas o vigilancia para monitorear las áreas de archivo.
- Establecimiento de medidas de seguridad contra incendios y otros riesgos físicos.

Gestión de Documentos Confidenciales:

Objetivo: Asegurar el manejo adecuado de documentos confidenciales y clasificados.

Procedimientos:

- Identificación clara de documentos confidenciales en la matriz de activos de información.
- Acceso restringido a personal específico autorizado por el profesional de gestión del área administrativa.
- Recomendaciones de manejo seguro durante la manipulación y el almacenamiento.

Registro de Acceso:

Objetivo: Mantener un registro detallado de todas las actividades de acceso para fines de auditoría y seguimiento.

Procedimientos:

- Registro de cada entrada y salida de personas autorizadas mediante planilla.
- Inclusión de detalles como fecha, hora, motivo de acceso y duración.
- Suministro de elementos de bio seguridad
- Almacenamiento seguro de los registros durante un período establecido.

En las instalaciones del centro de datos o de los centros de cableado no está permitido:

a. Ingresar sin previa autorización del profesional de gestión del área de Tecnologías de la Información y de las Comunicaciones.

b. Fumar, introducir alimentos o bebidas dentro del Data Center.

c. Mover, desconectar y/o conectar equipo de cómputo sin autorización escrita del líder del área de Tecnologías de la Información y de las Comunicaciones.

d. Realizar algún cambio en las conexiones o configuración sin previa autorización escrita del líder o profesional de gestión del área de Tecnologías de la Información y las Comunicaciones.

e. Alterar software instalado en los equipos sin autorización escrita del líder o profesional de gestión del área de Tecnologías de la Información y las Comunicaciones.

f. Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.

g. Extraer información de los equipos en dispositivos externos.

h. Toda persona que ingrese a hacer mantenimiento o dar soporte en los centros de cableado o centros de datos, debe hacer uso únicamente de los equipos y accesorios que les sean asignados, para los fines que haya autorizado por escrito el líder o profesional de gestión del área de Tecnologías de la Información y de las Comunicaciones.

Es responsabilidad del profesional de gestión del área de Tecnologías de la Información y de las Comunicaciones mantener almacenadas y en custodia las llaves de ingreso a los centros de cableado y data center. No está permitido sustraer o prestar dichas llaves sin autorización.

5.4 No repudio[4]

5.4.1 Trazabilidad

El área de Tecnologías de la Información y de las Comunicaciones verifica que los sistemas informáticos del COPNIA generen y mantengan trazabilidad apropiada con el fin de identificar usuarios y documentar las situaciones relacionadas con eventos de seguridad.

El área de Tecnologías de la Información y de las Comunicaciones será la encargada de asegurar que los sistemas de información cuenten con los registros requeridos para realizar la trazabilidad de las acciones ejecutadas en el sistema, garantizando los campos básicos de: Usuario, fecha, acción.

5.4.2 Retención

El periodo de retención de la información de las acciones realizadas por el usuario será el mismo que opere para el ciclo de vida de utilización del sistema de información mencionado, una vez el sistema de información sea dado de baja por obsolescencia, en los archivos de disposición final que se extraen del mencionado sistema para custodia en el archivo de la entidad, deberán también ser transferidos los registros de trazabilidad.

5.4.3 Auditoría

Garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

Es responsabilidad de la Oficina de Control Interno programar auditorías periódicas al cumplimiento de los lineamientos estipulados en el presente manual, conforme los procedimientos definidos para el proceso de Evaluación y Control de la entidad.

[4] La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción.

5.4.4 Intercambio electrónico de información

La información del COPNIA relacionada con la topología de la red, el direccionamiento interno, así como las configuraciones y demás datos relacionados con las redes y sistemas de comunicación de la entidad, deberá ser información confidencial.

Todo intercambio de información o interacción entre sistemas de información con otras entidades deberá estar soportado con un contrato o convenio formalizado y con el visto bueno del profesional de gestión del área de Tecnologías de la Información y de las Comunicaciones.

Cuando se requiera conectar la red o los sistemas de información del COPNIA con la red o sistemas de otra entidad, esta solicitud deberá ser estudiada y avalada por el profesional de gestión del área de Tecnologías de Información y de las Comunicaciones, incluyendo un análisis de los posibles riesgos asociados y posteriormente debe escalarse con la Dirección General para su respectiva aprobación, considerando siempre la necesidad de apoyar la misión del COPNIA.

El área de Tecnologías de la Información y de las Comunicaciones es responsable de proteger la información involucrada (transporte por protocolo seguro) en transacciones en línea, para evitar la transmisión incompleta, rutas equivocadas, alteración y divulgación.

El COPNIA establece los siguientes lineamientos para estos acuerdos o convenios de intercambio de información:

- El intercambio de información debe realizarse a través de protocolos seguros definidos por el profesional de gestión del área de Tecnologías de la Información y de las Comunicaciones de la entidad.
- El intercambio de información debe analizarse por un equipo interdisciplinar del COPNIA que conste como mínimo con los conceptos de aprobación de la sub dirección jurídica, área de contratación, área administrativa, oficina de seguridad y privacidad de la información, área de tecnologías de la información y las comunicaciones.

- La información que se suministrará del COPNIA a otra entidad, debe estar claramente detallada dentro del acuerdo o contrato, así como su disposición final y su tratamiento respectivo.

- Los repositorios finales de información, así como sus medios de trasmisión y presentación, deben contar con las características de seguridad exigidas por el profesional de gestión del Área de Tecnologías de la Información y las Comunicaciones.

- El consumo de información que se realiza al COPNIA, debe contar con las características técnicas y de seguridad que se dispongan por parte del profesional de gestión del Área de Tecnologías de la Información y las Comunicaciones, lo cual es dependiente de la arquitectura que maneje determinado sistema de información.

5.5 Antivirus

La Oficina de Seguridad y Privacidad de la Información del COPNIA establece lineamientos claros y precisos en relación con la gestión de antivirus para salvaguardar la integridad y confidencialidad de los datos. La implementación y mantenimiento de soluciones antivirus son considerados elementos cruciales en nuestra estrategia de seguridad cibernética.

El Área de Tecnologías de la Información y las Comunicaciones planificará y ejecutará las necesidades de recursos necesarios, que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

5.6 Privacidad y Confidencialidad[5]

El COPNIA desarrolla lineamientos y acciones orientadas a la protección y tratamiento de los datos personales recolectados para fines misionales, contractuales y administrativos. Dichos lineamientos se desarrollan en la Política de Protección de Datos personales y en el Manual para la Protección de Datos Personales disponibles en el sitio Web y en la documentación del proceso de Atención al Ciudadano.

El área de Gestión Humana es responsable de solicitar a funcionarios, supernumerarios y planta temporal la firma de acuerdos de confidencialidad individuales en los que se comprometan a no divulgar información interna y externa que conozcan en razón a la ejecución de actividades misional o desarrollo de labores administrativas. La firma del acuerdo implica que la información conocida por todo funcionario, en ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente.

El área de Contratación es responsable de incluir cláusulas de confidencialidad y no divulgación de tal forma que los proveedores de bienes o servicios se comprometan a no divulgar información interna y externa que conozca en razón a la ejecución de actividades misional o desarrollo de labores administrativas. La firma del acuerdo implica que la información conocida por todo contratista y/o tercero, en ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente.

[5] Este lineamiento contiene la descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente

5.7 Integridad[6]

Los líderes de las dependencias y áreas del COPNIA son responsables porque toda la información verbal, física o electrónica, sea entregada o transmitida integralmente, sin modificaciones o alteraciones, al destinatario correspondiente.

Es responsabilidad de todos los funcionarios del COPNIA hacer uso de los activos de información de forma responsable, profesional, ética y legal.

Es responsabilidad de todos los funcionarios del COPNIA, mantener la privacidad de las comunicaciones personales, en un nivel de servicio apropiado a la función que desempeñan en la entidad.

La información generada y recibida en el COPNIA, debe ser usada para los propósitos misionales de la Entidad, conforme a las funciones propias de cada cargo y para responder requerimientos de entes de control o terceros, de acuerdo con procedimientos definidos para tal fin.

En el caso de vinculación contractual, el compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de cláusula de integridad de la información. Es responsabilidad del Área de Contratación de la Subdirección Administrativa y Financiera, verificar la existencia de dicha cláusula.

5.8 Disponibilidad del Servicio e Información[7]

La Oficina de Seguridad y Privacidad de la Información establece los lineamientos para abordar las posibles indisponibilidades de la plataforma tecnológica de la entidad, en su ejercicio de evaluación de riesgos digitales, reconociendo la importancia crítica de garantizar la continuidad operativa y la integridad de los servicios. Se implementarán medidas proactivas para prevenir interrupciones, tales como respaldos en los sistemas clave, monitoreo constante de la infraestructura y evaluaciones periódicas de la capacidad y la recuperación (Ver ANEXO 2. Programación de Revisión de Backups para COPNIA sobre la Plataforma Tecnológica).

---

[6] Se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los funcionarios y/o terceros que hacen parte de la Entidad.

[7] Contiene los lineamientos que le permiten a la Entidad asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información.

El área de Tecnologías de la Información y de las Comunicaciones es responsable de implementar las medidas necesarias para disminuir los posibles efectos de las interrupciones en los sistemas de información o el normal funcionamiento de la infraestructura tecnológica; de igual forma, será la encargada de liderar la implementación de controles para asegurar la continuidad de los procesos críticos.

5.9 Registro y Auditoría[8]

Es responsabilidad del Área de Tecnologías de la información y de las Comunicaciones verificar que los sistemas de información almacenen los registros de cualquier evento de seguridad, así como de establecer un adecuado mecanismo para la gestión de los eventos de seguridad y reportar de ser necesario cualquier situación anómala que afecte los pilares de la disponibilidad, integridad y confidencialidad de la información a la oficina de seguridad y privacidad de la información.

Los registros de trazabilidad del sistema serán suministrados a la Oficina de Control Interno, según lo requiera en el marco de las auditorias anuales que se realizan a los procesos de la entidad.

5.10 Gestión de Incidentes de Seguridad de la Información[9]

Es deber de los funcionarios reportar, a través del procedimiento Atención de Incidencias y Requerimientos, TIC- pr-01, todo incidente de seguridad de información que atente en contra de las políticas consignadas en el presente documento o que identifique un riesgo o evento factible para la integridad, disponibilidad y seguridad de la información del COPNIA.

Es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones categorizar el incidente como "Seguridad de la información" y tomará las acciones respectivas para eliminar o mitigar la amenaza y adicional reportar de forma inmediata a la oficina de seguridad y privacidad de la información de la entidad. De ser necesario, el área de Tecnologías de la Información y de las Comunicaciones convocará al Subcomité de Seguridad de la Información para el análisis del incidente reportado.

[8] Esta política vela por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.

[9] Documenta los lineamientos para la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.

5.11 Capacitación y Sensibilización en Seguridad de la Información[10]

La Subdirección Administrativa y Financiera, a través del área de Gestión Humana, es responsable de incorporar en el Plan Institucional de Capacitación programas de uso y apropiación del presente manual, de tal manera que se promueva la apropiación de este, mediante una adecuada sensibilización, capacitación y comunicación.

5.12 Implementación de proyectos tecnológicos

Para la implementación de proyectos tecnológicos se requiere seguir los siguientes lineamientos:

- La arquitectura debe ser definida y aprobada por el Área de Tecnologías de la Información y de las Comunicaciones y revisada y avalada por la oficina de seguridad y privacidad de la información.

- El modelo de seguridad (protocolos, transacciones, implementación de roles, perfiles, arquitectura, autenticación y autorización, entre otros) debe ser definido por el área de Tecnologías de la Información y de las Comunicaciones, y revisada y avalada por la oficina de seguridad y privacidad de la información acorde con la protección de los activos de información y su criticidad.

- El proceso de implementación de los proyectos tecnológicos debe ser acordado con el Área de Tecnologías de la Información y de las Comunicaciones, acorde con la segregación de ambientes (desarrollo, pruebas, producción) y revisado y avalado por la oficina de seguridad y privacidad de la información.

- Las estrategias de migración y de salida a producción deben ser acordadas con el Área de Tecnologías de la Información y de las Comunicaciones, dependencia garante de minimizar los impactos y responsable de certificar la calidad de los productos entregados y revisado y avalado por la oficina de seguridad y privacidad de la información.

6. ANEXOS

6.1 SPI-fr-01 Declaración de Aplicabilidad para Seguridad y Privacidad de la Información
6.2 SPI-fr-02 programación de Actualizaciones para COPNIA Sobre la Plataforma Tecnológica
6.3 SPI-fr-03 Programación de Revisión de Backups para COPNIA sobre la Plataforma Tecnológica

[10] Lineamientos cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

7. CONTROL DE CAMBIOS

No.	Fecha	Descripción del cambio o modificación
1	Julio 2019	Primera emisión
2	Mayo 2023	Actualización del capítulo 2. Marco Institucional. Ajuste en la sección 5.3.2 Suministro del control de acceso
3	Enero 2024	Se incluyen conceptos en términos y definiciones; se incluyen responsabilidades de la Oficina de Seguridad y Privacidad de la Información; se incluyen las políticas de: Implementación de BitLocker para la Encripción de Equipos de Cómputo para Usuarios Finales, Objetivos de Punto de Recuperación (RPO) y Objetivos de Tiempo de Recuperación (RTO) de 24 Horas para los sistemas de información, Revisión y Mantenimiento de Matriz de Roles y Perfiles, Autenticación de Doble Factor (MFA) a través de Correo Electrónico y/o Mensaje de Texto al Celular, y Asignación y Uso de Derechos de Acceso Privilegiado. Se incluyen los anexos: Anexo 1-PROGRAMACION DE ACTUALIZACIONES PARA COPNIA SOBRE LA PLATAFORMA TECNOLOGICA; Anexo 2-PROGRAMACION DE REVISION DE BACKUPS PARA COPNIA SOBRE LA PLATAFORMA TECNOLOGICA; y anexo 3. SPI-fr-01 Declaración de Aplicabilidad. Teniendo en cuenta el objetivo del presente manual, se traslada al proceso de Seguridad y Privacidad de la Información como SPI-m-01 Manual de Seguridad de la Información V3, a cargo de la Oficina de Seguridad y Privacidad de la Información.

ALVARO IVAN TORRES GONZALEZ Firmado digitalmente por ALVARO IVAN TORRES GONZALEZ Fecha: 2024.02.06 19:40:14 -05'00'	JOHANNA TRINIDAD CANON LONDONO Firmado digitalmente por JOHANNA TRINIDAD CANON LONDONO	ANGELA PATRICIA ALVAREZ LEDESMA Firmado digitalmente por ANGELA PATRICIA ALVAREZ LEDESMA	RUBEN DARIO OCHOA ARBELAEZ Firmado digitalmente por RUBEN DARIO OCHOA ARBELAEZ
ÁLVARO IVÁN TORRES GONZÁLEZ	**JOHANNA CAÑON LONDOÑO**	**ÁNGELA PATRICIA ALVAREZ LEDESMA**	**RUBÉN DARÍO OCHOA ARBELÁEZ**
Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información	Profesional de gestión (E) del área de Tecnologías de la Información y de las Comunicaciones	Subdirectora de Planeación, Control y Seguimiento	Director General
ELABORÓ	**REVISÓ**	**REVISÓ**	**APROBÓ**

COPNIA	**DECLARACIÓN DE APLICABILIDAD (DDA) PARA SEGURIDAD DE LA INFORMACIÓN COPNIA**	**Versión:**	1
		Fecha del análisis	
		Día / **Mes**	**Año**

Se emite la presente declaración de aplicabilidad de controles para el Sistema de Gestión de Seguridad de la Información - SGSI, en función a la Oficina de seguridad y privacidad de la informacion COPNIA, como responsable de implementar, operar, mantener y mejorar el SGSI, para determinar los resultados de la identificación y valoración de riesgos de seguridad de la información, así como la formulación de actividades de tratamiento de riesgos, que cada líder operativo de proceso ha estimado convenientes, para mitigarlos y operar de forma segura y conforme los requisitos de los servicios ofrecidos por la entidad.

Los controles aplicables para la operación del Sistema de Gestión de Seguridad de la Información en la entidad son los numerales que se relacionan a continuación, tramitado con base en los 114 controles recomendados por la norma NTC/ISO 27001:2013.

La presente declaración de aplicabilidad será revisada conjuntamente con los resultados de cada nuevo proceso de valoración de riesgos y/o ante cambios significativos de los elementos de la plataforma tecnológica y/o de personal.

Esta información será material de comparación en los procesos de revisión por la dirección del SGSI, en los periodos convenidos para su actualización.

Lineamientos	
1	El lineamiento se cumple
0	El lineamiento no se cumple

CRITERIOS			**ANÁLISIS**		**APLICABLE PARA LA ENTIDAD**
ID DEL CONTROL	**NOMBRE DEL CONTROL**	**REQUISITO DEL CONTROL**	**Verificación**	**Evidencia**	
A.5 Políticas de seguridad de la información					
A.5.1 Orientación de la dirección para la seguridad de la información					
Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.					
A.5.1.1	Políticas para la seguridad de la información	*Control* La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información.			
A.5.1.2	Revisión de las políticas de seguridad de la información	*Control* Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continuas.			
A.6 Organización de la seguridad de la información					
A.6.1 Organización interna					
Objetivo: Establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.					
A.6.1.1	Roles y responsabilidades de la seguridad de la información	*Control* Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas.			
A.6.1.2	Segregación de funciones	*Control* Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización.			
A.6.1.3	Contacto con autoridades	*Control* Se deben mantener los contactos apropiados con las autoridades pertinentes.			
A.6.1.4	Contacto con grupos especiales de interés	*Control* Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales.			
A.6.1.5	Seguridad de la información en la gestión de proyecto	*Control* Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto.			
A.6.2 Dispositivos móviles y trabajo remoto					
Objetivo: garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles.					
A.6.2.1	Política de dispositivos móviles	*Control* Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos presentados al usar dispositivos móviles.			
A.6.2.2	Trabajo remoto	*Control* Se debe implementar una política y medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.			
A.7 Seguridad ligada a los recursos humanos					
A.7.1 Previo al empleo					
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sea aptos para los roles para los cuales están siendo considerados.					
A.7.1.1	Selección	*Control* Se debe realizar la verificación de antecedentes en todos los candidatos al empleo, de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos.			
A.7.1.2	Términos y condiciones de la relación laboral	*Control* Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de la organización en cuanto a seguridad de la información.			
A.7.2 Durante el empleo					
Objetivo: Asegurar que los empleados y contratistas estén en conocimiento y cumplan con sus responsabilidades de seguridad de la información.					
A.7.2.1	Responsabilidades de la dirección	*Control* La dirección debe solicitar a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.			
A.7.2.2	Concientización, educación y formación en seguridad de la información	*Control* Todos los empleados de la organización, y en donde sea pertinente, los contratistas deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su función laboral.			
A.7.2.3	Proceso disciplinario	*Control* Debe existir un proceso disciplinario formal y sabido por los empleados para tomar acciones en contra de los empleados que hayan cometido una infracción a la seguridad de la información.			
A.7.3 Desvinculación y cambio de empleo					
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo.					
A.7.3.1	Responsabilidades en la desvinculación o cambio de empleo	*Control* Se deben definir y comunicar las responsabilidades y funciones de la seguridad de la información que siguen en vigor después de la desvinculación o cambio de relación laboral.			
A.8 Administración de activos					
A.8.1 Responsabilidad por los activos					
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección pertinentes.					
A.8.1.1	Inventario de activos	*Control* Los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos.			
A.8.1.2	Propiedad de los activos	*Control* Los activos que se mantienen en inventario deben pertenecer a un dueño.			
		Control			

A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información.			
A.8.1.4	Devolución de activos	*Control* Todos los empleados y usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo.			
A.8.2 Clasificación de la información					
Objetivo: Asegurar que la información recibe el nivel de protección adecuado, según su importancia para la organización.					
A.8.2.1	Clasificación de la información	*Control* La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad para la divulgación o modificación sin autorización.			
A.8.2.2	Etiquetado de la información	*Control* Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo al esquema de clasificación de información adoptado por la organización.			
A.8.2.3	Manejo de activos	*Control* Se deben desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización.			
A.8.3 Manejo de los medios					
Objetivo: Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios.					
A.8.3.1	Gestión de los medios removibles	*Control* Se deben implementar los procedimientos para la gestión de los medios removibles, de acuerdo al esquema de clasificación adoptado por la organización.			
A.8.3.2	Eliminación de los medios	*Control* Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales			
A.8.3.3	Transferencia física de medios	*Control* Los medios que contengan información se deben proteger contra acceso no autorizado, uso inadecuado o corrupción durante el transporte.			
A.9 Control de acceso					
A.9.1 Requisitos de negocio para el control de acceso					
Objetivo: Restringir el acceso a la información y a las instalaciones de procesamiento de información.					
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso basadas en los requisitos del negocio y de seguridad de la información.			
A.9.1.2	Accesos a las redes y a los servicios de la red	*Control* Los usuarios solo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente.			
A.9.2 Gestión de acceso del usuario					
Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios.					
A.9.2.1	Registro y cancelación de registro de usuario	*Control* Se debe implementar un proceso de registro y cancelación de registro de usuario para habilitar la asignación de derechos de acceso.			
A.9.2.2	Asignación de acceso de usuario	*Control* Debe existir un procedimiento formal de asignación de acceso de usuario para asignar o revocar los derechos de acceso para todos los tipos de usuarios, a todos los sistemas y servicios.			
A.9.2.3	Gestión de derechos de acceso privilegiados	*Control* Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.			
A.9.2.4	Gestión de información secreta de autenticación de usuarios	*Control* Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal.			
A.9.2.5	Revisión de los derechos de acceso de usuario	*Control* Los propietarios de activos deben revisar los derechos de acceso de los usuarios de manera periódica.			
A.9.2.6	Eliminación o ajuste de los derechos de acceso	*Control* Se deben retirar los derechos de acceso de todos los empleados y usuarios externos a la información y a las instalaciones de procesamiento de información, una vez que termine su relación laboral, contrato o acuerdo o se ajuste según el cambio.			
A.9.3 Responsabilidades del usuario					
Objetivo: Responsabilizar a los usuarios del cuidado de su información de autenticación.					
A.9.3.1	Uso de información de autenticación secreta	*Control* Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta.			
A.9.4 Control de acceso al sistema y aplicaciones					
Objetivo: Evitar el acceso sin autorización a los sistemas y aplicaciones.					
A.9.4.1	Restricción de acceso a la información	*Control* Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso.			
A.9.4.2	Procedimientos de inicio de sesión seguro	*Control* Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro.			
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.			
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en capacidad de anular el sistema y los controles de aplicación.			
A.9.4.5	Control de acceso al código fuente de los programas	*Control* Se debe restringir el acceso al código fuente de los programas.			
A.10 Criptografía					
A.10.1 Controles criptográficos					
Objetivo: Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información.					
A.10.1.1	Política sobre el uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.			
		Control			

		DECLARACIÓN DE APLICABILIDAD (DDA) PARA SEGURIDAD DE LA INFORMACIÓN COPNIA	Versión:	1
			Fecha del análisis	
			Día	Mes	Año
A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil.			
A.11 Seguridad física y del ambiente					
A.11.1 Áreas seguras					
Objetivo: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información de la organización.					
A.11.1.1	Perímetro de seguridad física	*Control* Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen ya sea información sensible o crítica y las instalaciones de procesamiento de información.			
A.11.1.2	Controles de acceso físico	*Control* Las áreas seguras deben estar protegidas por controles de entrada apropiados que aseguren que solo se permite el acceso a personal autorizado.			
A.11.1.3	Seguridad de oficinas, salas e instalaciones	*Control* Se debe diseñar y aplicar la seguridad física en oficinas, salas e instalaciones.			
A.11.1.4	Protección contra amenazas externas y del ambiente	*Control* Se debe diseñar y aplicar la protección física contra daños por desastre natural, ataque malicioso o accidentes.			
A.11.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras.			
A.11.1.6	Áreas de entrega y carga	*Control* Se deben controlar los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones, y si es posible, aislarlas de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.			
A.11.2 Equipamiento					
Objetivo: Prevenir pérdidas, daños, hurtos o el compromiso de los activos así como la interrupción de las actividades de la organización.					
A.11.2.1	Ubicación y protección del equipamiento	*Control* El equipamiento se debe ubicar y proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.			
A.11.2.2	Elementos de soporte	*Control* Se debe proteger el equipamiento contra fallas en el suministro de energía y otras interrupciones causadas por fallas en elementos de soporte.			
A.11.2.3	Seguridad en el cableado	*Control* Se debe proteger el cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a servicios de información contra interceptación, interferencia o daños.			
A.11.2.4	Mantenimiento del equipamiento	*Control* El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad e integridad.			
A.11.2.5	Retiro de activos	*Control* El equipamiento, la información o el software no se deben retirar del local de la organización sin previa autorización.			
A.11.2.6	Seguridad del equipamiento y los activos fuera de las instalaciones	*Control* Se deben asegurar todos los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.			
A.11.2.7	Seguridad en la reutilización o descarte de equipos	*Control* Todos los elementos del equipamiento que contenga medios de almacenamiento deben ser revisados para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de su descarte o reutilización.			
A.11.2.8	Equipo de usuario desatendido	*Control* Los usuarios se deben asegurar de que a los equipos desatendidos se les da protección apropiada.			
A.11.2.9	Política de escritorio y pantalla limpios	*Control* Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.			
A.12 Seguridad de las operaciones					
A.12.1 Procedimientos operacionales y responsabilidades					
Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.					
A.12.1.1	Procedimientos de operación documentados	*Control* Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.			
A.12.1.2	Gestión de cambios	*Control* Se deben controlar los cambios a la organización, procesos de negocio, instalaciones de procesamiento de información y los sistemas que afecten la seguridad de la información.			
A.12.1.3	Gestión de la capacidad	*Control* Se debe supervisar y adaptar el uso de los recursos, y se deben hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.			
A.12.1.4	Separación de los ambientes de desarrollo, prueba y operacionales	*Control* Los ambientes para desarrollo, prueba y operación se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación.			
A.12.2 Protección contra código malicioso					
Objetivo: Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso.					
A.12.2.1	Controles contra código malicioso	*Control* Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios.			
A.12.3 Respaldo					
Objetivo: Proteger en contra de la pérdida de datos.					
A.12.3.1	Respaldo de la información	*Control* Se deben hacer copias de respaldo y pruebas de la información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada.			
A.12.4 Registro y monitoreo					
Objetivo: Registrar eventos y generar evidencia.					
A.12.4.1	Registro de evento	*Control* Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, faltas y eventos de seguridad de la información.			
	Protección de la información	*Control*			

COPNIA	DECLARACIÓN DE APLICABILIDAD (DDA) PARA SEGURIDAD DE LA INFORMACIÓN COPNIA	Versión:	1	
		Fecha del análisis		
		Día	Mes	Año
A.12.4.2	de registros	Las instalaciones de registro y la información de registro se deben proteger contra alteraciones y accesos no autorizados.			
A.12.4.3	Registros del administrador y el operador	*Control* Se deben registrar las actividades del operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad.			
A.12.4.4	Sincronización de relojes	*Control* Los relojes de todos los sistemas de procesamiento de información pertinente dentro de una organización o dominio de seguridad deben estar sincronizados a una sola fuente horaria de referencia.			
A.12.5 Control del software de operación					
Objetivo: Asegurar la integridad de los sistemas operacionales.					
A.12.5.1	Instalación del software en sistemas operacionales	*Control* Se deben implementar los procedimientos para controlar la instalación del software en los sistemas operacionales.			
A.12.6 Gestión de la vulnerabilidad técnica					
Objetivo: Evitar la explotación de las vulnerabilidades técnicas.					
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener la información acerca de las vulnerabilidades técnicas de los sistemas de información usados se debe obtener de manera oportuna, evaluar la exposición de la organización a estas vulnerabilidades y se deben tomar las medidas apropiadas para abordar el riesgo asociado.			
A.12.6.2	Restricciones sobre la instalación de software	*Control* Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.			
A.12.7 Consideraciones de la auditoría de los sistemas de información					
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.					
A.12.7.1	Controles de auditoría de sistemas de información	*Control* Los requisitos y las actividades de auditoría que involucran verificaciones de los sistemas operacionales se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones en los procesos del negocio.			
A.13 Seguridad de las comunicaciones					
A.13.1 Gestión de la seguridad de red					
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.					
A.13.1.1	Controles de red	*Control* Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones.			
A.13.1.2	Seguridad de los servicios de red	*Control* Los mecanismos de seguridad, los niveles del servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros.			
A.13.1.3	Separación en las redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes.			
A.13.2 Transferencia de información					
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.					
A.13.2.1	Políticas y procedimientos de transferencia de información	*Control* Las políticas, procedimientos y controles de transferencia formal deben estar en efecto para proteger la transferencia de la información mediante el uso de todos los tipos de instalaciones de comunicación.			
A.13.2.2	Acuerdos sobre transferencia de información	*Control* Los acuerdos deben abarcar la transferencia segura de la información del negocio entre la organización y terceros.			
A.13.2.3	Mensajería electrónica	*Control* La información involucrada en la mensajería electrónica debe ser debidamente protegida.			
A.13.2.4	Acuerdos de confidencialidad o no divulgación	*Control* Se deben identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de protección de la información de la organización.			
A.14 Adquisición, desarrollo y mantenimiento del sistema					
A.14.1 Requisitos de seguridad de los sistemas de información					
Objetivo: Asegurar que la seguridad de la información es parte integral de los sistemas de información en todo el ciclo. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios en las redes públicas.					
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Los requisitos relacionados a la seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes.			
A.14.1.2	Aseguramiento de servicios de aplicación en redes públicas	*Control* La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación y modificación no autorizada.			
A.14.1.3	Protección de las transacciones de servicios de aplicación	*Control* La información implicada en transacciones de servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.			
A.14.2 Seguridad en procesos de desarrollo y soporte					
Objetivo: Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información.					
A.14.2.1	Política de desarrollo seguro	*Control* Las reglas para el desarrollo de software y de sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización.			
A.14.2.2	Procedimientos de control de cambios del sistema	*Control* Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios.			
A.14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	*Control* Cuando se cambien las plataformas de operación, se deben revisar y poner a prueba las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.			
A.14.2.4	Restricciones en los cambios a los paquetes de software	*Control* Se debe desalentar la realización de modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, los que deben ser controlados de manera estricta.			

A.14.2.5	Principios de ingeniería de sistema seguro	*Control* Se deben establecer, documentar, mantener y aplicar los principios para los sistemas seguros de ingeniería para todos los esfuerzos de implementación del sistema de información.			
A.14.2.6	Entorno de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger los entornos de desarrollo seguro, de manera apropiada, para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de desarrollo del sistema.			
A.14.2.7	Desarrollo tercerizado	*Control* La organización debe supervisar y monitorear la actividad del desarrollo del sistema tercerizado.			
A.14.2.8	Prueba de seguridad del sistema	*Control* Durante el desarrollo se debe realizar la prueba de funcionalidad de seguridad			
A.14.2.9	Prueba de aprobación del sistema	*Control* Se deben definir los programas de prueba de aceptación y los criterios pertinentes para los nuevos sistemas de información, actualizaciones y versiones nuevas.			
A.14.3 Datos de prueba					
Objetivo: Asegurar la protección de los datos usados para prueba.					
A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba se deben seleccionar, proteger y controlar de manera muy rigurosa.			
A.15 Relaciones con el proveedor					
A.15.1 Seguridad de la información en las relaciones con el proveedor					
Objetivo: Asegurar la protección de los activos de la organización a los que tienen acceso los proveedores.					
A.15.1.1	Política de seguridad de la información para las relaciones con el proveedor	*Control* Se deben acordar y documentar, junto con el proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos de la organización.			
A.15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor	*Control* Todos los requisitos de seguridad de la información pertinente, deben ser definidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.			
A.15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones	*Control* Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados a los servicios de la tecnología de la información y las comunicaciones y la cadena de suministro del producto.			
A.15.2 Gestión de entrega del servicio del proveedor					
Objetivo: Mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos del proveedor.					
A.15.2.1	Supervisión y revisión de los servicios del proveedor	*Control* Las organizaciones deben supervisar, revisar y auditar la entrega del servicio del proveedor.			
A.15.2.2	Gestión de cambios a los servicios del proveedor	*Control* Se deben gestionar los cambios al suministro de los servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, al considerar la criticidad de la información del negocio, los sistemas y procesos involucrados y la reevaluación de los riesgos.			
A.16 Gestión de incidentes de seguridad de la información					
A.16.1 Gestión de incidentes de seguridad de la información y mejoras					
Objetivo: Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.					
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información.			
A.16.1.2	Informe de eventos de seguridad de la información	*Control* Se deben informar, lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados.			
A.16.1.3	Informe de las debilidades de seguridad de la información	*Control* Se debe requerir que los empleados y contratistas que usen los sistemas y servicios de información de la organización, observen e informen cualquier debilidad en la seguridad de la información en los sistemas o servicios, observada o que se sospeche.			
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben evaluar y decidir su van a ser clasificados como incidentes de seguridad de la información.			
A.16.1.5	Respuesta ante incidentes de seguridad de la información	*Control* Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados.			
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	*Control* Se debe utilizar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.			
A.16.1.7	Recolección de evidencia	*Control* La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia.			
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio					
A.17.1 Continuidad de la seguridad de la información					
Objetivo: Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad del negocio de la organización.					
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.			
A.17.1.2	Implementación de la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.			
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe verificar, de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas.			
A.17.2 Redundancias					
Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información					
	Disponibilidad de las	*Control*			

		DECLARACIÓN DE APLICABILIDAD (DDA) PARA SEGURIDAD DE LA INFORMACIÓN COPNIA	Versión:		1
			Fecha del análisis		
			Día	Mes	Año
A.17.2.1	Instalaciones de procesamiento de la información	Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia suficiente para cumplir con los requisitos de disponibilidad.			
A.18 Cumplimiento					
A.18.1 Cumplimiento con los requisitos legales y contractuales					
Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y todos los requisitos de seguridad.					
A.18.1.1	Identificación de la legislación vigente y los requisitos contractuales	*Control* Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.			
A.18.1.2	Derechos de propiedad intelectual	*Control* Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y al uso de productos de software patentados.			
A.18.1.3	Protección de los registros	*Control* Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.			
A.18.1.4	Privacidad y protección de la información de identificación personal	*Control* Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda.			
A.18.1.5	Regulación de los controles criptográficos	*Control* Se deben utilizar controles criptográficos que cumplan con todos los acuerdos, leyes, y regulaciones pertinentes.			
A.18.2 Revisiones de seguridad de la información					
Objetivo: Asegurar que la seguridad de la información se implemente y funcione de acuerdo a las políticas y procedimientos de la organización.					
A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos.			
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	*Control* Los gerentes deben revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes.			
A.18.2.3	Verificación del cumplimiento técnico	*Control* Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización.			

TOTAL DE CONTROLES A AUDITAR / EVALUAR	**114**
PORCENTAJE DE CUMPLIMIENTO NORMATIVO	**0%**
ÍTEMS CON NO CUMPLIMIENTO	**114**

Elaborado por:	**Revisado por:**	**Aprobado por:**
Nombre:	Nombre:	Nombre:
Cargo:	Cargo:	Cargo:

PROGRAMACIÓN DE ACTUALIZACIONES PARA COPNIA SOBRE LA PLATAFORMA TECNOLOGICA			
DESCRIPCIÓN	Las Actualizaciones Mensuales de Software del Consejo Profesional Nacional de Ingeniería COPNIA debe ser detallado y seguir un proceso cuidadosamente estructurado para garantizar la seguridad y el rendimiento de los sistemas informáticos de la Entidad.		
OBJETIVO	Asegurar que los sistemas de software utilizados por el Consejo Profesional Nacional de Ingeniería COPNIA estén actualizados, sean seguros y funcionen de manera eficiente, al tiempo que se minimizan los riesgos de interrupciones no planificadas.		
DESCRIPCIÓN DE ACTIVIDADES PARA ACTUALIZACIONES			
PASO	**ACTIVIDAD**	**DESCRIPCIÓN**	**VALIDACIÓN**
1	Identificación de Software y Componentes Clave	Enumerar todos los sistemas de software y componentes críticos que se utilizan en la entidad, incluyendo sistemas de gestión, bases de datos, aplicaciones web, software de ofimática, sistemas de seguridad, etc.	
2	Evaluación de Actualizaciones Disponibles	Monitorear mensualmente las fuentes de información oficiales del fabricante para conocer las actualizaciones de seguridad y las mejoras disponibles para los sistemas y componentes identificados.	
3	Priorización de Actualizaciones	Clasificar las actualizaciones en función de su criticidad acorde a las recomendaciones del fabricante del producto. Las actualizaciones de seguridad deben tener prioridad	
4	Planificación y Programación	Programar un día y una hora específicos para realizar las actualizaciones. Esto debe llevarse a cabo en un momento que minimice el impacto en las operaciones normales de la entidad.	
5	Creación de un Entorno de Pruebas	Antes de implementar actualizaciones en el entorno de producción, asegurar de crear un entorno de pruebas donde se puedan probar las actualizaciones y verificar su compatibilidad con otros sistemas.	
6	Verificación y Pruebas	Lleva a cabo pruebas exhaustivas en el entorno de pruebas para garantizar que las actualizaciones no causen problemas inesperados o incompatibilidades con otros sistemas	
7	Aseguramiento de Backups	Realizar las copias de seguridad de los sistemas y datos críticos antes de aplicar cualquier actualización.	
8	Implementación de Actualizaciones	Instalar las actualizaciones en el entorno de producción siguiendo las mejores prácticas.	
9	Documentación	Mantener registros detallados de todas las actualizaciones realizadas, incluyendo fechas, descripciones de las actualizaciones y problemas resueltos.	
10	Comunicación	Notificar a los usuarios, funcionarios de la Entidad y al personal del Área de Tecnologías de la Información y las Comunicaciones TIC sobre las actualizaciones programadas y cualquier posible interrupción en el servicio.	
11	Implementación en Producción	Una vez que las pruebas sean exitosas y las actualizaciones estén listas, se procede a implementarlas en el entorno de producción.	
12	Monitorización Post-Actualización	Supervisar el sistema después de la implementación de las actualizaciones para asegurarse de que todo funcione correctamente y de que no se hayan introducido nuevos problemas.	
13	Resolución de Problemas	Si surgen problemas inesperados, actuar rápidamente para resolverlos y, si es necesario, restaurar el sistema a su estado anterior utilizando las copias de seguridad.	
14	Evaluación Post-Actualización	Después de un período de tiempo, evaluar el impacto de las actualizaciones en términos de seguridad y rendimiento.	
15	Preparación para el Siguiente Ciclo de Actualización	Inmediatamente después de una actualización, comenzar a planificar y preparar el siguiente ciclo	

PERIODICIDAD DE ACTUALIZACIONES								
Meses	**Sistemas Misionales**	**Sistemas Documentales**	**Sistema ERP**	**Sistema de Nómina**	**Sistemas de Apoyo**	**Sistemas de Ofimática**	**Sistemas de Redes y Comunicaciones**	**Sistemas Operativos**
ENERO	Revisión Mensual			Mensual	Revisión Mensual		Mensual	Actualizaciones Automáticas
FEBRERO	Revisión Mensual	Bimestral		Mensual	Revisión Mensual	Bimestral	Mensual	Actualizaciones Automáticas
MARZO	Revisión Mensual			Mensual	Revisión Mensual		Mensual	Actualizaciones Automáticas
ABRIL	Revisión Mensual	Bimestral		Mensual	Revisión Mensual	Bimestral	Mensual	Actualizaciones Automáticas
MAYO	Revisión Mensual			Mensual	Revisión Mensual		Mensual	Actualizaciones Automáticas
JUNIO	Revisión Mensual	Bimestral	Semestral	Mensual	Revisión Mensual	Bimestral	Mensual	Actualizaciones Automáticas
JULIO	Revisión Mensual			Mensual	Revisión Mensual		Mensual	Actualizaciones Automáticas
AGOSTO	Revisión Mensual	Bimestral		Mensual	Revisión Mensual	Bimestral	Mensual	Actualizaciones Automáticas
SEPTIEMBRE	Revisión Mensual			Mensual	Revisión Mensual		Mensual	Actualizaciones Automáticas
OCTUBRE	Revisión Mensual	Bimestral		Mensual	Revisión Mensual	Bimestral	Mensual	Actualizaciones Automáticas
NOVIEMBRE	Revisión Mensual			Mensual	Revisión Mensual		Mensual	Actualizaciones Automáticas
DICIEMBRE	Revisión Mensual	Bimestral	Semestral	Mensual	Revisión Mensual	Bimestral	Mensual	Actualizaciones Automáticas

PROGRAMACION DE REVISION DE BACKUPS PARA COPNIA SOBRE LA PLATAFORMA TECNOLOGICA	
DESCRIPCIÓN	El objetivo de programar revisiones periódicas de backups es garantizar la integridad y disponibilidad de la información respaldada. Estas revisiones buscan verificar que los archivos almacenados en las copias de seguridad sean accesibles, estén completos y no hayan sufrido corrupciones. Al establecer un cronograma regular para estas revisiones, se puede identificar y corregir cualquier problema potencial antes de que sea necesario restaurar los datos. Esto contribuye a la fiabilidad del sistema de respaldo y asegura una rápida recuperación en caso de pérdida de datos.

DESCRIPCIÓN DE ACTIVIDADES PARA REVISIÓN DE BACKUPS

TIPO	FRECUENCIA BACKUP	FRECUENCIA REVISIÓN INTEGRIDAD	DESCRIPCIÓN	VALIDACIÓN
Backup de la Infraestructura Azure	Diaria	Diaria	Para garantizar que los datos respaldados en la infraestructura de Azure sean confiables y recuperables, se llevará a cabo una validación automática de los backups todos los días. Esto implica verificar la integridad de los archivos de backup y confirmar que se pueden restaurar de manera efectiva. Esto se realiza mediante la funcionalidad automática de respaldos Azure.	
Backups de Bases de Datos	Diaria	Mensual	Los backups de bases de datos se tomarán diariamente para asegurar la disponibilidad de datos críticos. Mensualmente, se llevará a cabo una revisión de integridad para verificar que los backups de bases de datos sean recuperables sin errores y se ajusten a las políticas de retención, a través de restauraciones completas en ambiente de pruebas.	
Backups de Configuraciones	Semestral	Anual	Los backups de configuraciones se realizarán cada seis meses para capturar la configuración actual del entorno. Sin embargo, la revisión de integridad de estos backups se realizará una vez al año. Esto implica asegurarse de que los backups de configuraciones sean legibles, completos y se puedan utilizar para restaurar la configuración de manera eficiente en caso de necesidad, mediante una restauración aleatoria sobre cada tipología de dispositivo y referencia, por ejemplo, un router de secretaria regional/seccional, un firewall, un AP etc.	

CONSIDERACIONES GENERALES

- Para todos los tipos de backups se verificará la integridad de los archivos respaldados.
- Se confirmará que los backups sean accesibles y se puedan restaurar con éxito.
- Se llevará un registro detallado de los resultados de las revisiones de integridad, creando un ticket de servicio para tal fin.
- En caso de encontrar problemas con la integridad de cualquier backup se tomarán las medidas correctivas necesarias, se informará por parte del área TIC al oficial de seguridad de la información y se documentarán.
- Se debe mantener una lista actualizada de todos los backups junto con sus fechas de toma y revisiones de integridad.
- Asegurarse de contar con procedimientos de restauración documentados para cada tipo de backup en caso de que sea necesario recuperar datos o configuraciones.

Meses	Backup de la Infraestruc	Backups de Bases de Datos	Backups de Configuraciones					
ENERO	Validación Automática Diaria	Validación Mensual	-					
FEBRERO	Validación Automática Diaria	Validación Mensual	-					
MARZO	Validación Automática Diaria	Validación Mensual	-					
ABRIL	Validación Automática Diaria	Validación Mensual	-					
MAYO	Validación Automática Diaria	Validación Mensual	-					
JUNIO	Validación Automática Diaria	Validación Mensual	-					
JULIO	Validación Automática Diaria	Validación Mensual	-					
AGOSTO	Validación Automática Diaria	Validación Mensual	-					
SEPTIEMBRE	Validación Automática Diaria	Validación Mensual	-					
OCTUBRE	Validación Automática Diaria	Validación Mensual	-					
NOVIEMBRE	Validación Automática Diaria	Validación Mensual	-					
DICIEMBRE	Validación Automática Diaria	Validación Mensual	Validación Anual					