REPÚBLICA DE COLOMBIA

COPNIA

Consejo Profesional Nacional de Ingeniería

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**2024 – 2026**

**TABLA DE CONTENIDO**

# 1 INTRODUCCIÓN

La información es un activo crítico en la actualidad y su seguridad y privacidad son fundamentales. Este plan de seguridad y privacidad de la información establece las bases para protegerla en el COPNIA, garantizando su confidencialidad, integridad y disponibilidad. En un mundo cada vez más digital y conectado, el Consejo Profesional Nacional de Ingeniería COPNIA, de acuerdo con su Política de Seguridad y Privacidad de la Información, se compromete con la implementación de un sistema de seguridad de la información que le permita responder por la integridad, disponibilidad y confidencialidad de esta, así como salvaguardar los datos de manera efectiva y cumplir con las regulaciones aplicables.

Conforme con lo establecido en el numeral 2.1.3 del Manual de Gobierno Digital, versión 6 emitida por MINTIC, el plan de seguridad y privacidad de la información precisa los detalles la manera en la que se realizará la implementación y mejora de la seguridad de la información en la Entidad para cada vigencia, en el que se estipulan directrices, tiempos y responsables, de tal manera que se logren resultados anuales mejores que en la vigencia anterior.

Es importante destacar que, en anteriores vigencias el COPNIA ha llevado a cabo diferentes actividades que han posibilitado el acceso, entre otros, a los siguientes beneficios:

- Contar con Matriz de Riesgos Digitales.
- Fortalecer la conciencia en cuanto a las amenazas y riesgos en el ciberespacio a los que se enfrentan los funcionarios en sus labores diarias.
- Cronograma para la implementación del Sistema de Gestión de Seguridad de la Información – SGSI.
- Establecer un proceso estratégico cuyo objetivo es proteger la información institucional.
- Contar con la olítica de Seguridad y Privacidad de la Información
- Contar con el Manual de Seguridad de la Información
- Contar con la Política de Gobierno Digital
- Contar con la Política de Gestión y Desempeño de Seguridad Digital
- Identificar riesgos que pueden afectar la seguridad de la información en los procesos de la Entidad.
- Establecer controles para asegurar las aplicaciones cuya infraestructura se encuentra alojada en la nube.
- Implementación del antivirus en plataforma *cloud*.
- Implementación de *firewalls* y VPN.
- Adopción de las tablas de control de acceso
- Registro de activos de información
- Índice de información reservada y clasificada

## 2. MARCO NORMATIVO

El marco normativo se toma como referencia en lo aplicable a la naturaleza jurídica del COPNIA, consignado en el portal web institucional en el siguiente link:

- Marco Normativo:

https://www.copnia.gov.co/nuestra-entidad/normatividad

## 3. MISIÓN Y VISIÓN DE LA ENTIDAD

Se toma como referencia en lo aplicable a la misión y visión consignados en el portal web institucional en los siguientes enlaces:

https://www.copnia.gov.co/nuestra-entidad/quienes-somos

**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. Resolución R2022039275 del 21 de octubre de 2022

**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. Resolución R2022039275 del 21 de octubre de 2022

**Objetivos estratégicos de la entidad:**

1. Mejorar la cobertura, oportunidad y calidad en la prestación de los servicios misionales.
2. Consolidar el Modelo de Gestión de la entidad para mejorar la prestación de los servicios misionales.
3. Fortalecer y articular las relaciones interinstitucionales y la comunicación con los diferentes grupos de interés de la Entidad.

https://www.copnia.gov.co/transparencia/plan-estrategico

## 4. OBJETIVO

Establecer las acciones estratégicas tendientes a fortalecer la seguridad y privacidad de la información en el Consejo Profesional Nacional de Ingeniería - COPNIA, mediante la planeación de actividades para la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI de la Entidad.

## 5. ALCANCE

El presente documento se encuentra articulado con el Plan Estratégico de Tecnologías de Información y de las Comunicaciones - PETIC (2023-2026).

El marco normativo se toma como referencia en lo aplicable a la naturaleza jurídica del COPNIA, así como la visión y visión consignados en el portal web institucional en los siguientes links:

## 6. DEFINICIONES

**ISO 27001:2013:** es un estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Su objetivo principal es proporcionar un marco estructurado para que las organizaciones implementen medidas de seguridad efectivas y gestionen de manera sistemática la protección de la información. La norma abarca aspectos como la evaluación de riesgos, la implementación de controles de seguridad, la gestión de incidentes y la mejora continua

**Sistema de Gestión de Seguridad de la Información (SGSI):** es un enfoque integral que busca salvaguardar la confidencialidad, integridad y disponibilidad de la información en una entidad. Basándose en normativas como la ISO 27001:2013, el SGSI implica la identificación y evaluación de riesgos, la implementación de controles adecuados, la gestión de incidentes de seguridad y la promoción de una cultura organizacional que valore la seguridad de la información.

**CSIRT del sector Gobierno**: El objetivo principal del CSIRT Gobierno, es ofrecer servicios proactivos, reactivos y de gestión de la seguridad básicos a todas las entidades del Estado, generando alertas y advertencias sobre amenazas y vulnerabilidades, realizando el tratamiento, análisis, respuesta y coordinación de incidentes, igualmente en el afianzamiento del conocimiento sobre seguridad, generando una cultura de seguridad digital en todos los funcionarios y encargados de seguridad digital surge como necesidad de realizar una adecuada gestión y reaccionar ante los incidentes cibernéticos de modo centralizado, para lo cual realiza seguimiento de manera unificada a las principales tipologías de ciberincidentes que atentan contra la defensa del Gobierno, para realizar de manera eficiente la gestión de sus riesgos.

**colCERT:** El Colcert es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, un equipo que es punto de contacto para coordinar la prevención, mitigación, gestión y respuesta ante incidentes de seguridad digital nacional tanto en el sector público como en el privado. Su objetivo es Coordinar con las instancias responsables de la Seguridad Digital, entre otros: el Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), y Sectoriales públicos y/o privados, la compartición de información, para la gestión de amenazas e incidentes de Seguridad Digital Nacional. También su objetivo es actuar como punto único de contacto y coordinación para responder de manera rápida y eficiente a incidentes y vulnerabilidades de Seguridad Digital que atenten o comprometan la Seguridad Digital Nacional.

**Infraestructura crítica cibernética:** se refiere a los sistemas y redes de tecnología de la información y comunicación que son esenciales para el funcionamiento y la seguridad de una nación. Estos sistemas son vitales para el funcionamiento de la sociedad, la economía y el gobierno. La infraestructura crítica cibernética incluye una amplia gama de sectores, como energía, agua, transporte, salud, finanzas, comunicaciones y servicios de emergencia.

**Ciberseguridad:** es el conjunto de prácticas, tecnologías y medidas diseñadas para proteger sistemas informáticos, redes y datos contra amenazas cibernéticas. Su objetivo principal es salvaguardar la confidencialidad, integridad y disponibilidad de la información digital, así como prevenir el acceso no autorizado, la manipulación y el robo de datos sensibles.

Esto implica la implementación de firewalls, antivirus, sistemas de detección de intrusiones y políticas de seguridad, así como la concientización y capacitación de usuarios para reducir riesgos asociados a la ingeniería social. Dada la creciente sofisticación de los ataques cibernéticos, la ciberseguridad es esencial tanto para individuos como para organizaciones, garantizando un entorno digital seguro y resistente frente a las amenazas en constante evolución.

**On-premise:** se refiere a la ubicación física de los recursos informáticos y software, indicando que están instalados y operan en el propio sitio o infraestructura de una organización en lugar de depender de servicios en la nube. En un entorno on-premise, las entidades mantienen y gestionan sus propios servidores, equipos de almacenamiento y aplicaciones en sus instalaciones. Esto ofrece un mayor control directo sobre la infraestructura y los datos, pero también implica la responsabilidad de mantener y actualizar hardware y software de manera local. Aunque el enfoque on-premise proporciona autonomía y cumplimiento normativo, puede tener costos iniciales y operativos más altos en comparación con soluciones basadas en la nube, que ofrecen flexibilidad y escalabilidad sin la necesidad de gestión física directa de la infraestructura.

**Firewall:** es una barrera de seguridad esencial en redes informáticas que actúa como un filtro entre una red privada y el flujo de datos que proviene de fuentes externas, como internet. Su función principal es monitorear, controlar y permitir o bloquear el tráfico de datos basándose en un conjunto de reglas predefinidas. Estas reglas determinan qué tipo de comunicación se permite o se deniega, contribuyendo así a prevenir accesos no autorizados, ataques cibernéticos y la propagación de malware. Los firewalls pueden implementarse tanto a nivel de hardware como de

software y son una herramienta fundamental para garantizar la seguridad y la integridad de una red al gestionar de manera efectiva el tráfico de información.

**Cisco Call Manager:** también conocido como Cisco Unified Communications Manager (CUCM), es una plataforma de software de administración de llamadas diseñada por Cisco Systems. Su función principal es facilitar y gestionar las comunicaciones unificadas en una red. CUCM permite integrar diversas aplicaciones de comunicación, como voz, video, mensajería y colaboración, en una única plataforma, brindando a las organizaciones la capacidad de mejorar la eficiencia y la productividad de sus comunicaciones. Este sistema administra funciones esenciales como el enrutamiento de llamadas, la asignación de recursos de comunicación, la administración de dispositivos y la implementación de servicios avanzados, ofreciendo así una solución integral para las necesidades de telefonía y colaboración.

**Controles criptográficos:** son medidas de seguridad implementadas para proteger la confidencialidad e integridad de la información mediante el uso de técnicas criptográficas. Estos controles involucran el empleo de algoritmos y protocolos criptográficos para cifrar datos, asegurando que solo las partes autorizadas puedan acceder a la información protegida. Además del cifrado, los controles criptográficos también abarcan la gestión adecuada de claves, que son esenciales para desbloquear y descifrar la información. La implementación efectiva de controles criptográficos desempeña un papel crucial en la seguridad de la información, ya que ayuda a salvaguardar datos sensibles frente a amenazas de acceso no autorizado y manipulación, contribuyendo así a mantener la confidencialidad y la integridad de la información en diversos contextos, como transacciones financieras, comunicaciones electrónicas y almacenamiento de datos críticos.

**Seguridad de endpoint:** se refiere a un enfoque de protección de sistemas informáticos que se centra en asegurar los dispositivos finales, como computadoras, portátiles, tabletas y dispositivos móviles, que se conectan a una red corporativa. Este enfoque implica la implementación de medidas y soluciones de seguridad específicas para prevenir, detectar y responder a posibles amenazas que puedan afectar estos puntos finales. Estas medidas pueden incluir antivirus, firewalls, detección de malware, control de aplicaciones y actualizaciones regulares de software. La seguridad de endpoint es esencial en el panorama actual de amenazas cibernéticas, ya que los dispositivos finales son puntos de entrada potenciales para ataques maliciosos. Un enfoque integral de seguridad de endpoint no solo protege los dispositivos individuales, sino que también contribuye a la seguridad general de la red, al limitar la propagación de amenazas y salvaguardar los datos almacenados y transmitidos desde y hacia estos puntos finales.

**Malware:** una contracción de "software malicioso", es un término que engloba diversos tipos de software diseñado con intenciones perjudiciales para sistemas informáticos y usuarios. Este software malicioso puede incluir virus, gusanos, troyanos, spyware, ransomware y otros programas dañinos. El propósito del malware puede variar, desde causar daño al sistema, robar información confidencial, hasta permitir el control remoto no autorizado del dispositivo afectado. Los métodos de distribución del malware son diversos e incluyen descargas maliciosas, correos

electrónicos de phishing y sitios web comprometidos. Para combatir el malware, se utilizan programas antivirus y otras soluciones de seguridad cibernética que buscan identificar, bloquear y eliminar estas amenazas antes de que causen daño. La constante evolución del malware exige una actualización continua de las medidas de seguridad para proteger eficazmente sistemas y datos contra estas amenazas.

**Ransomware:** es un tipo de software malicioso que cifra archivos en el sistema de una víctima, y luego exige un pago, generalmente en criptomonedas, a cambio de la clave necesaria para restaurar el acceso a esos archivos. Este tipo de ataque tiene el potencial de causar daños significativos, ya que puede afectar tanto a usuarios individuales como a organizaciones enteras, cifrando datos críticos y dejando a las víctimas en una situación comprometida. Los ataques de ransomware a menudo se distribuyen a través de correos electrónicos de phishing, sitios web maliciosos o mediante la explotación de vulnerabilidades en sistemas no actualizados. La prevención y la respuesta efectiva a los ataques de ransomware son fundamentales, y las medidas de seguridad como copias de seguridad regulares, actualizaciones de software y concientización sobre ciberseguridad son vitales para mitigar este tipo de amenaza.

**MFA o Autenticación Multifactor**: es una medida de seguridad que añade una capa adicional de protección a los sistemas informáticos y cuentas en línea. En lugar de depender únicamente de una contraseña, MFA requiere que los usuarios proporcionen múltiples formas de identificación para verificar su identidad. Esto puede incluir, por ejemplo, el uso de contraseñas tradicionales junto con códigos generados por una aplicación móvil, mensajes de texto, o dispositivos de seguridad físicos. Al incorporar varios factores de autenticación, MFA fortalece significativamente la seguridad al hacer más difícil para los atacantes comprometer una cuenta incluso si obtienen acceso a la contraseña. Esta práctica es ampliamente recomendada para proteger cuentas sensibles y reducir el riesgo de accesos no autorizados.

**Sistema Avanzado de Detección de Intrusiones (IDS):** son componentes esenciales en la seguridad cibernética que buscan identificar y responder a actividades maliciosas o anómalas en una red informática. Estos sistemas monitorean continuamente el tráfico de la red, analizando patrones y comportamientos para detectar posibles intrusiones o amenazas cibernéticas. Utilizando algoritmos avanzados y firmas de ataques conocidas, los IDS pueden identificar actividades sospechosas, como intentos de acceso no autorizado, patrones de tráfico inusuales o comportamientos maliciosos. Los IDS pueden desplegarse en el perímetro de la red, en servidores específicos o de manera distribuida en varios puntos de la infraestructura. Además de la detección, algunos IDS también pueden tomar medidas preventivas o alertar a los administradores de seguridad para que tomen acciones correctivas. Estos sistemas son fundamentales para fortalecer la postura de seguridad cibernética y mitigar los riesgos asociados con posibles amenazas e intrusiones.

**Sistema de Información y Eventos de Seguridad (SIEM):** son plataformas integrales diseñadas para recopilar, analizar y correlacionar datos de seguridad de diversas fuentes dentro de una infraestructura de tecnologías de la información. Estos sistemas permiten a las

organizaciones monitorear de manera proactiva la actividad en sus redes, sistemas y aplicaciones, identificando posibles amenazas y eventos de seguridad. Los SIEM recopilan información de registros (logs) generados por dispositivos, sistemas y aplicaciones, y aplican análisis avanzados para detectar patrones y comportamientos anómalos que podrían indicar actividades maliciosas. Además de la detección, los SIEM también ofrecen funciones de respuesta y generación de informes para facilitar la gestión eficaz de la seguridad. Al proporcionar una visión centralizada y en tiempo real de los eventos de seguridad, los SIEM desempeñan un papel crucial en el fortalecimiento de la postura de ciberseguridad de una organización y en la respuesta proactiva a posibles amenazas.

**Sistema de Prevención de Intrusiones (IPS):** son componentes críticos en la seguridad cibernética diseñados para detectar y prevenir amenazas informáticas mediante la inspección activa del tráfico de red en busca de patrones maliciosos o comportamientos anómalos. Estos sistemas operan de manera proactiva para bloquear o responder a posibles intrusiones, evitando que exploits y ataques maliciosos comprometan la integridad y seguridad de una red. Los IPS utilizan firmas y reglas predefinidas, así como análisis heurísticos avanzados, para identificar y detener actividades sospechosas, tales como intentos de explotación de vulnerabilidades o patrones de tráfico asociados con ataques conocidos. La implementación efectiva de un IPS fortalece la postura de seguridad de una organización, contribuyendo a mitigar riesgos y proteger activos digitales críticos contra amenazas cibernéticas.

**Red Privada Virtual (VPN):** es una tecnología que establece una conexión segura y cifrada entre dispositivos a través de una red pública, como internet. Esta conexión cifrada permite que los datos se transmitan de manera segura y privada, como si los dispositivos estuvieran directamente conectados a una red privada, incluso si están geográficamente separados. Las VPN son utilizadas principalmente para garantizar la privacidad y la seguridad de la comunicación en línea, especialmente en situaciones en las que se accede a información sensible o se requiere un acceso remoto a recursos de la entidad. Además, las VPN son valiosas para eludir restricciones geográficas y acceder a contenido en línea que podría estar limitado en ciertos lugares. Este tipo de conexión segura es esencial para proteger la información contra posibles amenazas y para garantizar una comunicación confiable en entornos digitales.

**Stakeholders:** en el ámbito de proyectos y de gestión, se refiere a todas las partes interesadas que pueden verse afectadas por las acciones, decisiones o resultados de una organización. Estas partes interesadas pueden incluir clientes, empleados, accionistas, proveedores, comunidades locales, reguladores y otros grupos que tienen un interés directo o indirecto en el éxito y las operaciones de la entidad. La gestión de relaciones con stakeholders implica la identificación, comprensión y consideración de las necesidades, expectativas y preocupaciones de estos grupos, con el objetivo de tomar decisiones que equilibren los intereses de todas las partes involucradas. Una gestión efectiva de stakeholders contribuye a construir relaciones sólidas y sostenibles, promoviendo la transparencia, la responsabilidad y la creación de valor compartido.

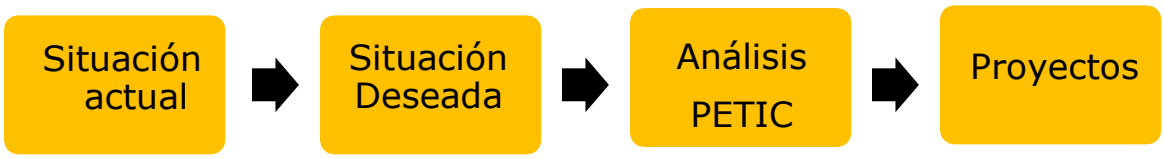
**Gestión de Parches y Actualizaciones:** es un proceso esencial en la seguridad informática que se centra en la planificación, implementación y seguimiento de actualizaciones y parches de software para mantener los sistemas y aplicaciones actualizados y seguros. Este enfoque busca remediar vulnerabilidades de seguridad conocidas al proporcionar correcciones y mejoras a medida que los fabricantes identifican y abordan posibles riesgos. La gestión efectiva de parches implica la evaluación periódica de las actualizaciones disponibles, la priorización de aquellas que son críticas para la seguridad, y la implementación de estos parches de manera oportuna para reducir la exposición a posibles amenazas. Este proceso ayuda a proteger los sistemas contra exploits y ataques que podrían aprovechar las debilidades no corregidas, fortaleciendo así la postura de seguridad cibernética de una organización o usuario individual.

**BitLocker:** es una herramienta de cifrado de disco integrada en los sistemas operativos de Microsoft, como Windows, que proporciona una capa adicional de seguridad al cifrar el contenido de las unidades de almacenamiento, como discos duros y unidades flash USB. Este mecanismo de cifrado ayuda a proteger la información almacenada en estos dispositivos, garantizando que solo usuarios autorizados con la clave correcta o el acceso adecuado puedan acceder a los datos. BitLocker utiliza algoritmos de cifrado fuertes y está diseñado para ser transparente para los usuarios, una vez que se ha configurado. Además, ofrece características como el cifrado de unidad completa o solo de sectores utilizados, y puede integrarse con Trusted Platform Module (TPM) para mejorar la seguridad del proceso de arranque del sistema operativo. BitLocker es especialmente útil en entornos compartidos o para usuarios individuales que buscan una capa adicional de protección para sus datos sensibles.

**Modelo de Seguridad y Privacidad de la Información – MSPI**: imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

## 7. METODOLOGÍA

Para definir los proyectos del presente plan, se analizó la situación actual vs. la deseada, buscando en todo momento una alineación con el PETIC. El resumen de la metodología se muestra a continuación:




En la metodología del plan de seguridad y privacidad de la información del COPNIA, el documento de aplicabilidad de cumplimiento de la norma ISO 27001/2013 (SOA Statement of Applicability) desempeña un papel esencial. Este documento identifica y evalúa los controles de seguridad de la información requeridos por la norma, adaptándolos a las necesidades y características específicas de la entidad. La ISO 27001/2013 establece estándares internacionales para la gestión de la seguridad de la información, y en su documento de aplicabilidad guía la implementación de medidas de seguridad con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de la información. Al integrar este documento en la metodología del plan de seguridad y privacidad de la información, la entidad puede asegurar una alineación efectiva con los requisitos normativos, proporcionando un marco estructurado para la gestión proactiva de los riesgos de seguridad y la protección de la información sensible. Este enfoque basado en ISO 27001/2013 contribuye a la creación de un programa de seguridad robusto y adaptado, fundamental para garantizar la integridad y seguridad de la información de la entidad.

## 8. SITUACIÓN ACTUAL

Respecto a los resultados en el análisis de brechas del Modelo de Seguridad y Privacidad de la Información – MSPI realizado en 2022, se encontró que es necesario atender las siguientes recomendaciones del MPSI (Modelo de privacidad y seguridad de la información):

- Fortalecer las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de socialización y promoción del uso del modelo de gestión de riesgos de seguridad digital convocadas por el Ministerio de Tecnologías de la Información y las Comunicaciones.

- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como registrarse en el CSIRT Gobierno y/o ColCERT.

- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al sub comité de seguridad de la información.

- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en

la entidad para ajustar dinámicamente las acciones de ciberseguridad.


De la gráfica anterior, se identifican aspectos por mejorar en los siguientes controles deseguridad de la información:

| Descripción | Criterio |
|---|---|
| No se cumplen los parámetros de seguridad en la cadena de suministro de la tecnología, en el sentido que se debe subir a una nube segura el *On Premise*, Firewall, servidores que están alojados localmente y que pueden contener información sensible, o establecer los controles necesarios para que la información sensible de la entidad no este expuesta a intrusiones. Lo que está pendiente es el Call Manager de Cisco, que se debe llevar a telefonía IP en la nube y los controles Biométricos. | La norma ISO 27001:2013 en su anexo A, control A.15.1.3 Cadena de suministro de la tecnología de información y comunicación |
| No todos los funcionarios aplican el requerimiento de claves seguras. | La norma ISO 27001:2013 en su anexo A, control A.9.4.3 Sistema de gestión de contraseñas: los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad. |

| Descripción | Criterio |
|---|---|
| No se evidencia que los propietarios de activos revisen los derechos de acceso de los usuarios de manera periódica. | La norma ISO 27001:2013 en su anexo A, control A.9.2.5 Revisión de los derechos de acceso de usuario: Los propietarios de activos deben revisar los derechos de acceso de los usuarios de manera periódica. |
| El Manual de la Seguridad de la Información, de código TIC-m-01 no hace referencia a los usuarios privilegiados. Se evidencia que no se restringe y controla la asignación y uso de los derechos de acceso privilegiado de manera adecuada | La norma ISO 27001:2013 en su anexo A, control A.9.2.3 Gestión de derechos de acceso privilegiados: Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado |
| Dentro de la información revisada no existe control de cambios | La norma ISO 27001:2013 en su anexo A, controles A.12.1.2 Gestión de cambios, A.14.2.2 Procedimientos de control de cambios del sistema y A.15.2.2 Gestión de cambios a los servicios del proveedor: Se deben controlar los cambios a la entidad, procesos de negocio, instalaciones de procesamiento de información y los sistemas que afecten la seguridad de la información.<br>• Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios.<br>• 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. |
| No se hacen restauraciones aleatorias de las copias de seguridad. | La norma ISO 27001:2013 en su anexo A, controles A.12.3.1 Respaldo de la información: 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. |

| Descripción | Criterio |
|---|---|
| No se evidencia una adecuada y oportuna gestión de las vulnerabilidades técnicas. | La norma ISO 27001:2013 en su anexo A, control A.12.6.1 Gestión de las vulnerabilidades técnicas: 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 entidad a estas vulnerabilidades y se deben tomar las medidas apropiadas para abordar el riesgo asociado.<br>a) la entidad debería definir y establecer los roles y las responsabilidades asociadas a la administración de vulnerabilidades técnicas, incluido el monitoreo de vulnerabilidades, la evaluación de riesgos de vulnerabilidad, los parches, el seguimiento de activos y cualquier tipo de responsabilidades de coordinación necesarias;<br>b) se deberían identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otras tecnologías (en base a la lista de inventario de activos, ver 8.1.1); estos recursos de información se deberían actualizar en base a los cambios en el inventario o cuando se encuentran nuevos recursos útiles;<br>c) se debería definir una línea de tiempo para reaccionar frente a las notificaciones de vulnerabilidades técnicas posiblemente relevantes;<br>d) una vez que se ha identificado una vulnerabilidad técnica, la entidad debería identificar los riesgos asociados y las medidas que se deberían tomar, dichas medidas podrían involucrar la aplicación de parches a los sistemas vulnerables o la aplicación de otros controles;<br>e) en función de la urgencia con la que se deba abordar una vulnerabilidad técnica, la medida tomada se debería realizar de acuerdo a los controles relacionados con la administración de cambios (ver 12.1.2) o siguiendo los procedimientos de respuesta ante incidentes de seguridad (ver 16.1.5);<br>f) si existe un parche disponible de una fuente legítima, se deberían evaluar los riesgos asociados a la instalación del parche (los riesgos que impone la vulnerabilidad se deberían comparar con el riesgo de instalar el parche);<br>g) los parches se pueden evaluar y probar antes de su instalación para garantizar que son eficaces y no involucran efectos colaterales que no se pueden tolerar; si no existen parches disponibles se deberían considerar otros controles como: |

| Descripción | Criterio |
|---|---|
| | 1) desactivar todos los servicios o capacidades relacionadas a la vulnerabilidad;<br>2) adaptar o agregar controles de acceso, es decir, firewalls, en las fronteras de la red (ver 13.1);<br>3) mayor monitoreo para detectar ataques reales;<br>4) concientizar sobre la vulnerabilidad;<br>h) se debería mantener un registro de auditoría para todos los procedimientos que se realizan;<br>i) el proceso de vulnerabilidad técnica se debería monitorear y evaluar regularmente para poder garantizar su efectividad y eficiencia;<br>j) se deberían abordar primero los sistemas en alto riesgo;<br>k) se debería alinear un proceso de administración de vulnerabilidades técnicas eficaz con actividades de administración de incidentes para comunicar los datos sobre vulnerabilidades con la función de respuesta ante incidentes y proporcionar los procedimientos técnicos en caso de que ocurra un incidente;<br>l) definir un procedimiento para abordar la situación donde se ha identificado una vulnerabilidad, pero donde no existe una contramedida. En esta situación, la entidad debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las medidas defectivas y correctivas adecuadas. |
| El Plan de Continuidad del negocio está en construcción a mediano plazo, lo que incide en un eventual incremento de la probabilidad de materialización de riesgos durante el periodo en que no se tenga plenamente desarrollado. | La norma ISO 27001:2013 en su anexo A, control A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio: Los controles de Planificación de la continuidad de la seguridad de la información, Implementación de la continuidad de la seguridad de la información, Verificación, revisión y evaluación de la continuidad de la seguridad de la información, así como las redundancias con Disponibilidad de las instalaciones de procesamiento de la información.<br>Una entidad debería determinar si la continuidad de la seguridad de la información se incluye dentro del proceso de administración de continuidad del negocio o dentro del proceso de administración de recuperación ante desastres. Se deberían determinar los requisitos de seguridad de la información al planificar la continuidad comercial y la recuperación ante desastres.<br>En la ausencia de una continuidad comercial formal y una planificación de recuperación ante desastres, la administración de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos ante situaciones |

| Descripción | Criterio |
|---|---|
| | adversas, en comparación con las condiciones operacionales normales. De manera alternativa, una entidad puede desarrollar un análisis de impacto comercial para los aspectos de seguridad de la información y determinar los requisitos de seguridad de la información que se aplican a situaciones adversas. |
| Se observan casos de alteración de Registros en el aplicativo BPM. | La norma ISO 27001:2013 en su anexo A, control A.18.1.3 Protección de los registros: 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 |
| Protección y privacidad de la información de carácter personal | Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicable. |
| Reglamentación de controles criptográficos | Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. |

## 9. SITUACIÓN DESEADA

El Consejo Profesional Nacional de Ingeniería – COPNIA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Para el COPNIA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

El Sistema de Gestión de Seguridad de la Información - SGSI debe cumplir con las siguientes premisas[1]:

i. Minimizar el riesgo en las funciones más importantes de la Entidad.
ii. Cumplir con los principios de seguridad de la información.

1 Basado en el documento https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

iii. Cumplir con los principios de la función administrativa.
iv. Mantener la confianza de funcionarios y ciudadanía.
v. Apoyar la innovación tecnológica.
vi. Proteger los activos tecnológicos.
vii. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
viii. Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, ciudadanos digitales, contratistas y demás partes interesadas del COPNIA
ix. Garantizar la continuidad del negocio frente a incidentes.
x. El COPNIA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen 12 principios [2]de seguridad que soportan el SGSI del COPNIA:

i. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada una de las partes interesadas.
ii. La entidad protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros.
iii. La entidad protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
iv. La entidad protegerá su información de las amenazas originadas por factores internos o externos.
v. La entidad protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
vi. La entidad controlará la operación de sus procesos misionales garantizando la seguridad de los recursos tecnológicos y las redes de datos.
vii. La entidad implementará control de acceso a la información, sistemas y recursos de red.
viii. La entidad garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
ix. La entidad garantizará 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.
x. La entidad garantizará la disponibilidad de sus procesos misionales y la continuidad de su operación basada en el impacto que pueden generar los eventos.
xi. La entidad garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

## 10. ANÁLISIS PETIC

[2] Basado en el documento https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Se requiere que el SGSI (Sistema de gestión de seguridad de la información) brinde el apoyo para el logro de los objetivos y necesidades en los proyectos cuyo propósito es poner a disposición de la Entidad una arquitectura tecnológicaque habilite el modelo ágil, que evolucione rápidamente según las necesidades funcionales, modelo de servicio de TI, ciberseguridad, innovación y nuevas tecnologías.

## 11. PROYECTOS ESPECÍFICOS 2024-2026

De acuerdo con el análisis metodológico planteado anteriormente para la generación de proyectos de seguridad de la información, se plantea lo siguiente:

1. Fortalecer la gestión de incidentes de seguridad incorporando un enfoque preventivo.
2. Implementar el programa de capacitación y sensibilización en seguridad de la información.
3. Fortalecer controles de seguridad de la información, según el análisis de brechas y la auditoría interna.
4. Apoyar las políticas de Protección de Datos Personales.
5. Implementar las estrategias de recuperación ante Desastres.
6. Apoyar y monitorear la implementación del plan de tratamiento de riesgos de seguridad de la Información.
7. Apoyo a los procesos de controles de seguridad en la nube.
8. Adopción de los controles de ISO 27001

Por lo tanto, la implementación del SGSI, proyectado dentro de la estrategia 2024-2026, es esencial para proteger los activos de información críticos, cumplir con regulaciones, gestionar riesgos, mejorar la confianza de las partes interesadas y garantizar la continuidad de los servicios misionales. Además, demuestra un compromiso de la Entidad con la seguridad de la información y contribuye a una gestión más eficiente y efectiva de los recursos relacionados con la seguridad.

Se plantean por parte de seguridad de la información, proyectos a implementar para mejorar la integridad disponibilidad y confidencialidad de la información. Por lo tanto, se presentan los proyectos fundamentales para la estrategia 2024-2026:

| **Nombre del proyecto** | **Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)** |
|---|---|
| **Descripción y contexto** | • El proyecto de Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) tiene como objetivo establecer un marco integral que salvaguarde la confidencialidad, integridad y disponibilidad de la información en una entidad. A través de este sistema, se pretende identificar y evaluar los riesgos asociados a la seguridad de la información, establecer controles y procedimientos adecuados, y fomentar una cultura organizacional orientada a la seguridad. La implementación del SGSI implica la definición de políticas, la asignación |

| **Nombre del proyecto** | **Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)** |
|---|---|
| | de responsabilidades, la realización de auditorías periódicas y la continua mejora del sistema, garantizando así una gestión proactiva y eficaz de la seguridad de la información en todas las áreas de la entidad. Este enfoque sistemático busca no solo cumplir con estándares y normativas, sino también fortalecer la resiliencia de la entidad frente a posibles amenazas y vulnerabilidades, asegurando la protección de la información vital para el desarrollo y éxito de la entidad. |
| **Fases del proyecto** | **1. Planificación:**<br><br>Diagnóstico Inicial: Evaluar el estado actual de la seguridad de la información en la entidad.<br>Definición de Alcance y Objetivos: Establecer los límites del SGSI y los resultados esperados.<br><br>**2. Análisis de Riesgos:**<br><br>Identificación de Activos: Enumerar y clasificar los activos de información críticos.<br>Evaluación de Riesgos: Analizar las amenazas y vulnerabilidades para determinar los riesgos asociados.<br><br>**3. Diseño:**<br><br>Desarrollo de Controles: Definir y diseñar los controles de seguridad necesarios.<br>Políticas y Procedimientos: Elaborar documentos que establezcan las reglas y procedimientos de seguridad.<br><br>**4. Implementación:**<br><br>Instalación de Controles: Poner en práctica los controles y medidas de seguridad definidos.<br>Capacitación y Concientización: Formar al personal sobre las políticas y prácticas de seguridad.<br><br>**5. Monitoreo y Evaluación:**<br><br>Auditorías Internas: Realizar auditorías para evaluar la eficacia del SGSI.<br>Gestión de Incidentes: Desarrollar procedimientos para manejar incidentes de seguridad.<br><br>**6. Mejora Continua:**<br><br>Revisión y Actualización: Evaluar regularmente el SGSI |

| Nombre del proyecto | Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) |
|---|---|
| | para asegurar su relevancia.<br>Acciones Correctivas y Preventivas: Tomar medidas para corregir problemas identificados y prevenir futuros incidentes.<br><br>**7. Certificación (opcional):**<br><br>Auditoría Externa: Contratar a una entidad certificadora para evaluar y certificar el SGSI según estándares reconocidos (por ejemplo, ISO 27001). |
| **Recursos** | Oficina de Seguridad y Privacidad de la Información |
| **Fecha Inicio estimada** | 2024 |
| **Fecha Fin estimada** | 2024 |

| Nombre del proyecto | Protección contra malware y ransomware |
|---|---|
| **Descripción y contexto** | • El proyecto de Protección contra malware y ransomware tiene como objetivo fortalecer la seguridad informática de la entidad mediante la implementación de soluciones especializadas. Se focaliza en la defensa contra amenazas tales como virus, malware y ataques de ransomware, a través de la adopción de medidas proactivas. Esto implica la instalación y configuración de soluciones de seguridad de endpoint avanzadas, que ofrecen una protección integral en los puntos finales de la red. Además, se implementarán mejoras en la infraestructura de firewall, estableciendo barreras sólidas para prevenir intrusiones no autorizadas. Con este enfoque estratégico, se busca garantizar la integridad, confidencialidad y disponibilidad de los datos, promoviendo un entorno digital seguro y resistente frente a las crecientes amenazas cibernéticas. |
| **Fases del proyecto** | **1. Evaluación de Riesgos y Necesidades:**<br><br>Análisis de Amenazas: Identificación de amenazas específicas de malware y ransomware.<br>Evaluación de Vulnerabilidades: Analizar puntos débiles en la infraestructura actual.<br><br>**2. Definición de Requerimientos:**<br><br>Especificaciones Técnicas: Establecer los criterios técnicos para las soluciones de seguridad.<br>Requisitos del Sistema: Definir los requisitos específicos |

| Nombre del proyecto | Protección contra malware y ransomware |
|---|---|
| | del sistema de seguridad.<br><br>**3. Selección de Soluciones:**<br><br>Elección de Herramientas: Seleccionar soluciones de seguridad de endpoint y firewall que se ajusten a los requisitos.<br>Contratación de Proveedores.<br><br>**4. Diseño e Integración:**<br><br>Planificación de Implementación: Elaborar un plan detallado para la implementación.<br>Configuración del Firewall: Establecer reglas y políticas de seguridad en el firewall.<br>Implementación de Soluciones de Endpoint: Instalar y configurar las soluciones de seguridad en los puntos finales.<br>**5. Pruebas y Validación:**<br><br>Simulación de Ataques: Realizar pruebas de seguridad simulando posibles escenarios de ataque.<br>Validación de la Configuración: Verificar que las soluciones de seguridad estén funcionando según lo esperado.<br>**6. Capacitación del Personal:**<br><br>Entrenamiento: Brindar capacitación al personal sobre el uso adecuado de las nuevas herramientas de seguridad.<br>Concientización sobre Seguridad: Educar al personal sobre las amenazas de malware y ransomware.<br>**7. Implementación y Despliegue:**<br><br>Instalación en Producción: Implementar las soluciones de seguridad en el entorno de producción.<br>Monitorización Inicial: Iniciar la monitorización continua de eventos de seguridad.<br>**8. Optimización y Ajustes:**<br><br>Ajustes Finos: Realizar ajustes en las configuraciones para optimizar el rendimiento.<br>Gestión de Incidentes: Establecer procedimientos para la gestión de incidentes de seguridad.<br>**9. Documentación:**<br><br>Documentación del Proyecto: Crear documentación detallada sobre la configuración y procedimientos.<br>Manuales de Usuario: Preparar manuales para el personal sobre el uso de las soluciones implementadas. |

| **Nombre del proyecto** | **Protección contra malware y ransomware** |
|---|---|
| **Recursos** | Oficina de Seguridad y Privacidad de la Información – Área de Tecnologías de las Información y de las Comunicaciones – TIC |
| **Fecha Inicio estimada** | 2024 |
| **Fecha Fin estimada** | 2025 |

| **Nombre del proyecto** | **Gestión de identidad y acceso** |
|---|---|
| **Descripción y contexto** | • El proyecto de Gestión de Identidad y Acceso tiene como objetivo fundamental fortalecer la seguridad y controlar de manera eficiente el acceso a los recursos de la entidad. A través de la implementación de soluciones de autenticación multifactor (MFA), se busca agregar capas adicionales de seguridad para verificar la identidad de los usuarios, mitigando así los riesgos asociados con la autenticación tradicional. Además, se propone la instauración de políticas de acceso basadas en roles, que permiten asignar privilegios de manera específica y contextual, garantizando que los usuarios solo tengan acceso a los recursos necesarios para sus funciones. Esta iniciativa no solo refuerza la protección contra posibles amenazas y violaciones de seguridad, sino que también optimiza la administración de identidades y simplifica la gestión de accesos, contribuyendo a un entorno informático más seguro, eficiente y alineado con las mejores prácticas de seguridad de la información. |
| **Fases del proyecto** | **1. Análisis y Evaluación:**<br><br>Evaluación de la Infraestructura Actual: Analizar la estructura de identidad y acceso existente.<br>Identificación de Necesidades: Determinar los requisitos específicos de autenticación y acceso de la entidad.<br>**2. Diseño de la Arquitectura:**<br><br>Definición de Políticas de Acceso: Establecer políticas basadas en roles para asignar privilegios.<br>Selección de Soluciones MFA: Identificar y elegir soluciones MFA adecuadas para la entidad.<br>**3. Desarrollo e Integración:**<br><br>Configuración de Políticas: Implementar y configurar políticas de acceso basadas en roles.<br>Integración de Soluciones MFA: Integrar las soluciones MFA con los sistemas existentes. |

| **Nombre del proyecto** | **Gestión de identidad y acceso** |
|---|---|
| | **4. Pruebas y Validación:**<br><br>Pruebas de Funcionalidad: Realizar pruebas para garantizar que las soluciones MFA y las políticas de acceso funcionen correctamente.<br>Validación de Seguridad: Verificar la seguridad y eficacia de las nuevas medidas implementadas.<br>**5. Implementación Gradual:**<br><br>Despliegue Faseado: Implementar la gestión de identidad y acceso en fases, para minimizar impactos y asegurar una transición suave.<br>Capacitación del Personal: Proporcionar capacitación a los usuarios y al personal de TI sobre las nuevas políticas y procedimientos.<br>**6. Monitorización Continua:**<br><br>Supervisión del Acceso: Establecer sistemas de monitorización para vigilar el acceso de los usuarios.<br>Análisis de Registros: Revisar y analizar registros de acceso para identificar posibles anomalías.<br>**7. Optimización y Ajustes:**<br><br>Ajustes en Políticas: Realizar ajustes en las políticas de acceso según la retroalimentación y cambios en la entidad.<br>Mejora Continua: Identificar oportunidades de mejora y optimización del sistema de gestión de identidad y acceso. |
| **Recursos** | Oficina de Seguridad y Privacidad de la Información – Área de Tecnologías de la Información y de las Comunicaciones – TIC |
| **Fecha Inicio estimada** | 2024 |
| **Fecha Fin estimada** | 2024 |

| **Nombre del proyecto** | **Escaneo de vulnerabilidades en la arquitectura tecnológica de la entidad** |
|---|---|
| **Descripción y contexto** | • El proyecto de Escaneo de Vulnerabilidades en la arquitectura tecnológica de la entidad tiene como objetivo la mejora continua de la seguridad mediante la realización de evaluaciones periódicas. Estas evaluaciones buscan identificar y mitigar amenazas y vulnerabilidades en la infraestructura tecnológica de la entidad. A través de escaneos de vulnerabilidades exhaustivos, se pretende analizar la robustez de los sistemas y aplicaciones, proporcionando una visión detallada de los posibles riesgos. Este enfoque proactivo permite implementar medidas correctivas y preventivas, |

| **Nombre del proyecto** | **Escaneo de vulnerabilidades en la arquitectura tecnológica de la entidad** |
|---|---|
| | fortaleciendo la postura de seguridad y reduciendo la exposición a posibles ataques. La implementación de un ciclo constante de escaneo y mejora refuerza la resiliencia de la entidad frente a las amenazas cibernéticas en un entorno tecnológico en constante evolución. |
| **Fases del Proyecto** | **1. Planificación:**<br><br>Definición de Objetivos: Establecer metas específicas para la evaluación de vulnerabilidades.<br>Alcance del Proyecto: Delimitar el alcance de los sistemas, redes o aplicaciones a evaluar.<br>Recolección de Información:<br><br>Inventario de Activos: Identificar y catalogar todos los activos tecnológicos relevantes.<br>Revisión de Arquitectura: Analizar la estructura tecnológica y su interconexión.<br>**2. Configuración del Escaneo:**<br><br>Selección de Herramientas: Elegir las herramientas de escaneo de vulnerabilidades más adecuadas.<br>Configuración de Parámetros: Establecer los parámetros y criterios de escaneo.<br>**3. Escaneo Inicial:**<br><br>Ejecución de Herramientas: Realizar el escaneo inicial de vulnerabilidades en la arquitectura.<br>Recopilación de Resultados: Obtener y analizar los resultados del escaneo.<br>**4. Análisis de Riesgos:**<br><br>Priorización de Vulnerabilidades: Clasificar y priorizar las vulnerabilidades identificadas.<br>Evaluación de Impacto: Analizar el impacto potencial de las vulnerabilidades en la entidad.<br>Desarrollo de Plan de Mitigación:<br><br>Definición de Medidas Correctivas: Establecer acciones específicas para abordar las vulnerabilidades.<br>Asignación de Responsabilidades: Designar responsabilidades para la implementación de medidas correctivas.<br>**5. Implementación de Soluciones:**<br><br>Aplicación de Parches: Realizar actualizaciones y aplicar parches de seguridad según sea necesario.<br>Configuración de Seguridad: Ajustar la configuración de sistemas y aplicaciones para mitigar vulnerabilidades. |

| Nombre del proyecto | Escaneo de vulnerabilidades en la arquitectura tecnológica de la entidad |
|---|---|
| | **6. Escaneo Post-Mitigación:**<br><br>Realización de Segundo Escaneo: Ejecutar un segundo escaneo para verificar la efectividad de las medidas implementadas.<br>Validación de Resultados: Confirmar que las vulnerabilidades han sido adecuadamente mitigadas.<br>**7. Documentación y Reporte:**<br><br>Informe de Vulnerabilidades: Documentar los hallazgos, medidas tomadas y resultados de los escaneos.<br>Recomendaciones para Mejoras Continuas: Proporcionar recomendaciones para fortalecer la seguridad a largo plazo.<br>**8. Seguimiento Continuo:**<br><br>Implementación de Monitoreo Continuo: Establecer sistemas de monitoreo continuo para identificar nuevas vulnerabilidades.<br>Ciclo de Mejora Continua: Evaluar periódicamente la efectividad de las medidas de seguridad y ajustar según sea necesario. |
| **Recursos** | Oficina de Seguridad y Privacidad de la Información – Área de Tecnologías de la Información y de las Comunicaciones – TIC |
| **Fecha Inicio estimada** | 2024 |
| **Fecha Fin estimada** | 2026 |

| Nombre del proyecto | Monitorización y detección de amenazas |
|---|---|
| **Descripción y contexto** | • El proyecto de Monitorización y Detección de Amenazas tiene como objetivo fortalecer la seguridad de la entidad mediante la implementación de sistemas avanzados de detección de intrusiones (IDS) y sistemas de información y eventos de seguridad (SIEM). Estas soluciones permitirán monitorear de manera proactiva la red y los sistemas, identificando patrones y comportamientos anómalos que puedan indicar posibles amenazas. La integración de IDS proporciona una primera línea de defensa al identificar actividades maliciosas, mientras que el SIEM centraliza y analiza los eventos de seguridad, facilitando una respuesta inmediata a incidentes. Esta iniciativa busca dotar a la entidad de la capacidad para detectar y responder a amenazas en tiempo real, mejorando la postura de seguridad |

| Nombre del proyecto | Monitorización y detección de amenazas |
|---|---|
| | y asegurando la continuidad operativa frente a los desafíos constantes del panorama cibernético. |
| **Fases del Proyecto** | **1. Planificación y Análisis:**<br><br>Evaluación de Requerimientos: Identificación de las necesidades específicas de monitorización y detección de amenazas.<br>Definición de Objetivos: Establecimiento de metas claras y medibles para el proyecto.<br>**2. Diseño de la Arquitectura:**<br><br>Selección de Tecnologías: Elección de soluciones IDS y SIEM adecuadas para los requisitos de la entidad.<br>Diseño de la Infraestructura: Planificación de la configuración y distribución de los sistemas de detección.<br>**3. Implementación de IDS:**<br><br>Despliegue de Sensores: Instalación y configuración de sensores IDS en la red.<br>Configuración de Reglas y Firmas: Definición de reglas y firmas para la detección de intrusiones específicas.<br>**4. Implementación de SIEM:**<br><br>Integración con Fuentes de Datos: Conexión del SIEM con diferentes fuentes de datos, como registros de sistemas y aplicaciones.<br>Configuración de Correlación de Eventos: Establecimiento de reglas de correlación para identificar patrones de eventos sospechosos.<br>**5. Pruebas y Validación:**<br><br>Simulación de Incidentes: Realización de pruebas para evaluar la eficacia de la detección y respuesta a incidentes simulados.<br>Validación de Configuración: Verificación de que los sistemas IDS y SIEM estén configurados correctamente.<br>**6. Capacitación del Personal:**<br><br>Formación en el Uso de Herramientas: Capacitación del personal en la operación de las herramientas IDS y SIEM.<br>Desarrollo de Procedimientos de Respuesta: Creación de procedimientos para la respuesta a incidentes.<br>**7. Despliegue Gradual:**<br><br>Implementación por Fases: Despliegue gradual de los sistemas de monitorización y detección para minimizar |

| **Nombre del proyecto** | **Monitorización y detección de amenazas** |
|---|---|
| | impactos.<br>Monitoreo Inicial: Inicio del monitoreo y ajuste inicial de parámetros.<br>**8. Optimización y Ajustes Continuos:**<br><br>Ajustes de Configuración: Realización de ajustes en la configuración según la retroalimentación y el análisis de resultados.<br>Mejora Continua: Identificación de oportunidades para mejorar la eficacia de la detección y respuesta.<br>**9. Documentación y Reporte:**<br><br>Creación de Documentación: Elaboración de documentación detallada sobre la configuración y el funcionamiento de los sistemas implementados.<br>Informe de Incidentes: Documentación de incidentes detectados y acciones tomadas. |
| **Recursos** | Oficina de Seguridad y Privacidad de la Información – Área de Tecnologías de la Información y de las Comunicaciones – TIC |
| **Fecha Inicio estimada** | 2024 |
| **Fecha Fin estimada** | 2026 |

| **Nombre del proyecto** | **Cifrado de datos** |
|---|---|
| **Descripción y contexto** | • El proyecto se enfoca en la implementación efectiva de seguridad mediante BitLocker, una solución de cifrado de datos integral. Se busca garantizar la confidencialidad de la información almacenada mediante el cifrado de datos en reposo en dispositivos de almacenamiento, como discos duros y unidades USB. Mediante la integración de BitLocker, se establecerá una capa adicional de protección para prevenir el acceso no autorizado a los datos almacenados en dispositivos de almacenamiento físico. Además, se asegurará la seguridad en tránsito mediante la configuración adecuada de políticas y prácticas recomendadas, proporcionando una defensa integral que abarca desde la creación hasta el transporte de los datos. Este enfoque integral con BitLocker fortalecerá la seguridad de los datos, proporcionando una sólida barrera contra amenazas y garantizando la integridad y privacidad de la información sensible. |

| Nombre del proyecto | Cifrado de datos |
|---|---|
| **Fases del proyecto** | **1. Planificación:**<br><br>Definición de objetivos y requisitos específicos.<br>Identificación de los recursos necesarios, incluyendo hardware y software.<br>Evaluación de la infraestructura existente y posibles impactos en los sistemas existentes.<br>Desarrollo de un plan de proyecto detallado con cronograma y asignación de recursos.<br>**2. Diseño:**<br><br>Selección y configuración de la solución BitLocker de acuerdo con los requisitos del proyecto.<br>Definición de políticas de cifrado y acceso.<br>Evaluación y mitigación de posibles riesgos de implementación.<br>Diseño de procedimientos para la gestión de claves de cifrado.<br>**3. Implementación:**<br><br>Instalación y configuración de BitLocker en los sistemas designados.<br>Despliegue gradual del cifrado en dispositivos de almacenamiento específicos.<br>Capacitación del personal en cuanto a las nuevas políticas y procedimientos de seguridad.<br>Realización de pruebas de funcionamiento y verificación de la correcta implementación.<br>**4. Gestión de Cambios:**<br><br>Monitoreo continuo de la implementación para identificar posibles problemas o ajustes necesarios.<br>Gestión de cambios según sea necesario para abordar problemas emergentes o ajustar la configuración según las necesidades.<br>**5. Evaluación de la Seguridad:**<br><br>Realización de auditorías de seguridad para evaluar la efectividad del cifrado implementado.<br>Identificación y corrección de posibles vulnerabilidades.<br>Verificación de cumplimiento con normativas y políticas internas.<br><br>**6. Documentación:**<br><br>Creación de documentación detallada sobre la configuración de BitLocker y las políticas de seguridad implementadas.<br>Desarrollo de procedimientos operativos estándar (SOP) para la gestión continua de la seguridad de datos.<br>**7. Mantenimiento y Mejora Continua:** |

| **Nombre del proyecto** | **Cifrado de datos** |
|---|---|
| | Implementación de procesos para el monitoreo continuo y la gestión de actualizaciones de seguridad.<br>Evaluación periódica de la eficacia de las medidas de seguridad implementadas.<br>Mejora continua de las políticas y procedimientos en función de las lecciones aprendidas y los cambios en el entorno de seguridad. |
| **Recursos** | Oficina de Seguridad y Privacidad de la Información – Área de Tecnologías de la Información y de las Comunicaciones - TIC |
| **Fecha Inicio estimada** | 2024 |
| **Fecha Fin estimada** | 2025 |

| **Nombre del proyecto** | **Gestión de parches y actualizaciones** |
|---|---|
| **Descripción y contexto** | • El proyecto se enfoca en la implementación de una sólida Gestión de Parches y Actualizaciones con el objetivo de mantener los sistemas y aplicaciones de la entidad actualizados con los últimos parches de seguridad. Se establecerá un proceso integral que abarque la identificación proactiva de vulnerabilidades, la evaluación de la criticidad de los parches disponibles y la implementación eficiente de actualizaciones. Se diseñarán políticas y procedimientos para coordinar las actividades de parcheo, minimizando el impacto en la operación diaria mientras se maximiza la seguridad del entorno tecnológico. Además, se incorporarán mecanismos de monitoreo continuo para garantizar la eficacia del proceso y se proporcionará capacitación al personal para fomentar una cultura de seguridad que reconozca la importancia de mantener los sistemas al día con las últimas medidas de protección. Este enfoque integral busca fortalecer la postura de seguridad de la entidad, reduciendo riesgos y mitigando posibles amenazas derivadas de vulnerabilidades no parcheadas. |
| **Fases del Proyecto** | **1. Planificación:**<br><br>Definición de los objetivos específicos del proyecto.<br>Identificación de los sistemas y aplicaciones críticos que requieren actualizaciones regulares.<br>Evaluación de las políticas de parches actuales y análisis de posibles mejoras. |

| Nombre del proyecto | Gestión de parches y actualizaciones |
|---|---|
| | Establecimiento de un equipo de gestión de parches y asignación de responsabilidades.<br>**2. Inventario y Evaluación:**<br><br>Creación de un inventario detallado de sistemas y aplicaciones.<br>Evaluación de las vulnerabilidades existentes y la criticidad de los sistemas.<br>Identificación de los proveedores y fuentes para obtener información sobre parches de seguridad.<br>**3. Diseño del Proceso:**<br><br>Desarrollo de políticas y procedimientos para la gestión de parches.<br>Establecimiento de un proceso de prueba para evaluar la compatibilidad y estabilidad de los parches antes de la implementación.<br>Definición de cronogramas y ventanas de mantenimiento para minimizar el impacto en la productividad.<br>**4. Implementación:**<br><br>Configuración de herramientas de gestión de parches y actualizaciones.<br>Desarrollo de un plan de implementación que incluya la secuencia adecuada de parches.<br>Realización de pruebas piloto en entornos controlados antes de la implementación a gran escala.<br>**5. Monitoreo y Control:**<br><br>Implementación de herramientas de monitoreo para evaluar la efectividad de las actualizaciones y detectar posibles problemas.<br>Establecimiento de alertas para notificar sobre la falta de actualizaciones o posibles fallos en el proceso.<br>Revisión continua de métricas de seguridad y cumplimiento.<br>**6. Documentación:**<br><br>Creación de documentación detallada sobre políticas, procedimientos y resultados de pruebas.<br>Desarrollo de procedimientos operativos estándar (SOP) para la gestión continua de parches y actualizaciones.<br>**7. Capacitación y Concientización:**<br><br>Implementación de programas de capacitación para el personal sobre la importancia de las actualizaciones de seguridad.<br>Fomento de una cultura de seguridad que promueva la colaboración en la aplicación de parches y la comunicación de problemas de seguridad.<br>**8. Revisión y Mejora Continua:** |

| **Nombre del proyecto** | **Gestión de parches y actualizaciones** |
|---|---|
| | Evaluación periódica del proceso de gestión de parches para identificar áreas de mejora.<br>Incorporación de retroalimentación del equipo y del monitoreo continuo para ajustar y mejorar el proceso.<br>Actualización constante de las políticas y procedimientos en función de las lecciones aprendidas y las evoluciones del entorno de seguridad. |
| **Recursos** | Oficina de seguridad y privacidad de la información – Área de Tecnologías de la Información y de las Comunicaciones - TIC |
| **Fecha Inicio estimada** | 2024 |
| **Fecha Fin estimada** | 2026 |

| **Nombre del proyecto** | **Seguridad en la nube** |
|---|---|
| **Descripción y contexto** | • El proyecto se centra en fortalecer la seguridad en la nube dentro del ecosistema tecnológico de la entidad mediante la implementación de soluciones y políticas específicas. Se buscará establecer una seguridad perimetral robusta que proteja los datos y sistemas en entornos de nube, con el objetivo de incrementar los niveles de privacidad, confidencialidad y disponibilidad de la información. Esto implicará la selección e implementación de herramientas y servicios de seguridad en la nube, así como la definición de políticas que aborden aspectos como la gestión de accesos, el cifrado de datos, la monitorización continua y la respuesta a incidentes. Al integrar estas medidas, se pretende crear un entorno en la nube altamente seguro, mitigando riesgos y asegurando la integridad de la información sensible de la entidad. |
| **Fases del proyecto** | **1. Evaluación y Planificación:**<br>• Identificación de los activos críticos y datos sensibles almacenados en la nube.<br>• Evaluación de la infraestructura y servicios en la nube existentes.<br>• Definición de objetivos de seguridad y requisitos específicos.<br>• Desarrollo de un plan estratégico que incluya la selección de soluciones de seguridad en la nube y la planificación de la implementación.<br>**2. Selección de Soluciones y Herramientas:**<br>• Investigación y selección de herramientas y |

| Nombre del proyecto | Seguridad en la nube |
|---|---|
| | servicios de seguridad en la nube que se alineen con los requisitos del proyecto.<br>• Evaluación de proveedores y soluciones para asegurar la integración y compatibilidad adecuadas con la infraestructura existente.<br>**3. Diseño de la Arquitectura de Seguridad:**<br>• Desarrollo de una arquitectura de seguridad en la nube que incluya medidas como cortafuegos, sistemas de detección de intrusiones, gestión de identidades y acceso, y cifrado de datos.<br>• Definición de políticas de seguridad que aborden aspectos específicos de la nube, como la gestión de claves y la privacidad de los datos.<br>**4. Implementación Gradual:**<br>• Implementación escalonada de las soluciones y políticas de seguridad en la nube.<br>• Configuración y prueba de las medidas de seguridad para garantizar su eficacia.<br>• Capacitación del personal en las nuevas políticas y procedimientos de seguridad.<br>**5. Gestión de Identidades y Accesos:**<br>• Implementación de controles de acceso y autenticación robustos.<br>• Configuración de políticas de gestión de identidades para garantizar que solo los usuarios autorizados tengan acceso a los recursos en la nube.<br>**6. Monitorización Continua:**<br>• Implementación de herramientas de monitorización y registro de eventos en la nube.<br>• Establecimiento de alertas para identificar y responder rápidamente a posibles amenazas o incidentes de seguridad.<br>**7. Evaluación de Riesgos y Mejora Continua:**<br>• Realización de evaluaciones periódicas de riesgos para identificar posibles vulnerabilidades.<br>• Actualización y mejora continua de las medidas de seguridad en función de las lecciones aprendidas y la evolución de las amenazas.<br>**8. Documentación y Cumplimiento:**<br>• Creación de documentación detallada sobre la arquitectura de seguridad, políticas y procedimientos.<br>• Verificación del cumplimiento con estándares y regulaciones relevantes. |

| **Nombre del proyecto** | **Seguridad en la nube** |
|---|---|
| **Recursos** | Oficina de seguridad y privacidad de la información – Área de Tecnologías de la Información y de las Comunicaciones - TIC |
| **Fecha Inicio estimada** | 2024 |
| **Fecha Fin estimada** | 2024 |

| **Nombre del proyecto** | **Pruebas de penetración** |
|---|---|
| **Descripción y contexto** | • El proyecto consiste en la ejecución de pruebas de penetración periódicas con el objetivo de evaluar la resistencia de los sistemas y aplicaciones ante posibles ataques. Se llevarán a cabo análisis exhaustivos de la infraestructura tecnológica, identificando vulnerabilidades y puntos débiles que podrían ser explotados por actores maliciosos. Las pruebas se realizarán siguiendo metodologías reconocidas, simulando escenarios realistas de amenazas para evaluar la efectividad de las medidas de seguridad existentes. Los resultados de estas pruebas permitirán la implementación de acciones correctivas y la mejora continua de las defensas, fortaleciendo así la postura de seguridad de la entidad frente a posibles ciberataques y garantizando la protección integral de los activos de información. |
| **Fases del proyecto** | **1. Planificación:**<br>• Definición de los objetivos y alcance de las pruebas de penetración.<br>• Identificación de sistemas y aplicaciones a evaluar.<br>• Establecimiento de acuerdos de participación y comunicación con los stakeholders.<br>• Desarrollo de un plan detallado que incluya el cronograma, los métodos de prueba y las herramientas a utilizar.<br>**2. Reconocimiento:**<br>• Recopilación de información sobre la infraestructura, sistemas y aplicaciones a evaluar.<br>• Identificación de posibles puntos de entrada y vulnerabilidades mediante análisis de información pública y pasiva.<br>**3. Exploración:**<br>• Utilización de herramientas automatizadas para identificar activos y servicios en la red.<br>• Escaneo de vulnerabilidades para detectar posibles |

| Nombre del proyecto | Pruebas de penetración |
|---|---|
| | brechas de seguridad.<br>**4. Análisis de Vulnerabilidades:**<br>• Evaluación detallada de las vulnerabilidades identificadas durante la fase de exploración.<br>• Clasificación de las vulnerabilidades según su gravedad y posibles impactos.<br>**5. Explotación:**<br>• Intento controlado de aprovechar las vulnerabilidades identificadas para ganar acceso no autorizado.<br>• Validación de la existencia de vulnerabilidades y determinación de su explotabilidad.<br>**6. Post-Explotación:**<br>• Análisis de los sistemas comprometidos para evaluar el alcance del acceso no autorizado.<br>• Identificación de posibles movimientos laterales y escalada de privilegios.<br>**7. Informe de Resultados:**<br>• Documentación detallada de todas las actividades realizadas y los hallazgos obtenidos.<br>• Clasificación de las vulnerabilidades según su criticidad.<br>• Recomendaciones específicas para mitigar y corregir las vulnerabilidades identificadas.<br>**8. Revisión y Validación de Correcciones:**<br>• Seguimiento de las acciones correctivas implementadas por el equipo de seguridad.<br>• Validación de la efectividad de las medidas correctivas y mitigación de riesgos.<br>**9. Entrenamiento y Concientización:**<br>• Capacitación del personal para fortalecer la conciencia de seguridad.<br>• Desarrollo de prácticas recomendadas y pautas para evitar vulnerabilidades comunes.<br>**10. Mejora Continua:**<br>• Evaluación periódica de los procesos de pruebas de penetración y ajuste de las metodologías según las lecciones aprendidas.<br>• Actualización de políticas de seguridad y procedimientos en función de la evolución de las amenazas. |
| **Recursos** | Oficina de seguridad y privacidad de la información – Área de Tecnologías de la Información y de las Comunicaciones – TIC |

| **Nombre del proyecto** | **Pruebas de penetración** |
|---|---|
| **Fecha Inicio estimada** | 2025 |
| **Fecha Fin estimada** | 2026 |

| **Nombre del proyecto** | **Seguridad en equipos de computo** |
|---|---|
| **Descripción y contexto** | • El proyecto se enfoca en fortalecer la seguridad en equipos de cómputo mediante la implementación de políticas y soluciones específicas. Se establecerán medidas como el uso de VPN para asegurar comunicaciones seguras, el cifrado de datos para proteger la confidencialidad de la información almacenada en los dispositivos y la implementación de una sólida gestión de equipos de cómputo para garantizar la aplicación consistente de políticas de seguridad. Estas medidas se diseñarán considerando la diversidad de dispositivos en la entidad, abordando amenazas potenciales y promoviendo buenas prácticas de seguridad entre los usuarios. Con un enfoque integral, el proyecto tiene como objetivo mitigar riesgos, proteger la integridad de la información y fortalecer la postura de seguridad en los equipos de cómputo de la entidad. |
| **Fases del proyecto** | **1. Evaluación y Análisis de Riesgos:**<br>• Identificación de activos críticos y evaluación de riesgos asociados.<br>• Análisis de las amenazas y vulnerabilidades específicas para los equipos de cómputo.<br>**2. Definición de Políticas de Seguridad:**<br>• Desarrollo de políticas de seguridad que aborden el uso de VPN, cifrado de datos y gestión de equipos.<br>• Establecimiento de directrices claras sobre el manejo seguro de la información y el acceso a los recursos.<br>**3. Selección de Soluciones Tecnológicas:**<br>• Investigación y selección de soluciones de VPN adecuadas para la entidad.<br>• Implementación de herramientas de cifrado de datos que se integren con los dispositivos de cómputo utilizados.<br>• Evaluación y elección de soluciones de gestión de equipos que permitan la aplicación efectiva de las políticas de seguridad.<br>**4. Desarrollo de Procedimientos Operativos:** |

| **Nombre del proyecto** | **Seguridad en equipos de computo** |
|---|---|
| | • Creación de procedimientos operativos estándar (SOP) para el uso de VPN, la aplicación de cifrado y la gestión segura de equipos.<br>• Capacitación del personal en los nuevos procedimientos y políticas.<br>**5. Implementación de Soluciones:**<br>• Despliegue e integración de las soluciones tecnológicas seleccionadas en los equipos de cómputo.<br>• Configuración de políticas de seguridad en las herramientas implementadas.<br>• Realización de pruebas para asegurar la correcta funcionalidad de las soluciones.<br>**6. Monitoreo y Gestión Continua:**<br>• Implementación de mecanismos de monitoreo para supervisar el uso de VPN, el estado del cifrado y la gestión de equipos.<br>• Establecimiento de alertas para detectar posibles violaciones de seguridad o eventos inusuales.<br>• Gestión continua de equipos, incluyendo actualizaciones de software, parches y auditorías de seguridad.<br>**7. Evaluación de la Efectividad:**<br>• Realización de evaluaciones periódicas para medir la efectividad de las políticas y soluciones implementadas.<br>• Recopilación de métricas de seguridad y cumplimiento.<br>**8. Capacitación y Concientización Continua:**<br>• Desarrollo de programas de capacitación continua para mantener al personal informado sobre las mejores prácticas de seguridad.<br>• Fomento de la conciencia de seguridad entre los usuarios.<br>**9. Revisión y Mejora Continua:**<br>• Evaluación regular de la postura de seguridad y ajuste de políticas y soluciones según sea necesario.<br>• Incorporación de lecciones aprendidas de incidentes de seguridad y cambios en el entorno tecnológico. |
| **Recursos** | Oficina de seguridad y privacidad de la información – Área de Tecnologías de la Información y de las Comunicaciones – TIC |

| **Nombre del proyecto** | **Seguridad en equipos de computo** |
|---|---|
| **Fecha Inicio estimada** | 2024 |
| **Fecha Fin estimada** | 2026 |

| **Nombre del proyecto** | **Protección de la red** |
|---|---|
| **Descripción y contexto** | • El proyecto se centra en fortalecer la seguridad de la red mediante la implementación de medidas clave. Se llevará a cabo la instalación de firewalls robustos para controlar y monitorear el tráfico de red, estableciendo reglas y políticas de filtrado para prevenir accesos no autorizados. Además, se implementará la segmentación de red, dividiendo la infraestructura en zonas aisladas para limitar la propagación de posibles amenazas. La incorporación de sistemas de prevención de intrusiones (IPS) reforzará aún más las defensas, detectando y respondiendo de manera proactiva a intentos de intrusiones en tiempo real. Este enfoque integral tiene como objetivo crear una red más resistente y segura, reduciendo riesgos y protegiendo los activos de información crítica de la entidad contra posibles amenazas cibernéticas. |
| **Fases del proyecto** | **1. Evaluación y Análisis de la Red:**<br>• Identificación de activos críticos y análisis de la topología de la red.<br>• Evaluación de vulnerabilidades existentes y amenazas potenciales.<br>• Recopilación de requisitos específicos para la protección de la red.<br>**2. Definición de Políticas de Seguridad:**<br>• Desarrollo de políticas de seguridad de red que aborden el filtrado de tráfico, la segmentación y la prevención de intrusiones.<br>• Establecimiento de reglas y directrices para el uso seguro de la red.<br>**3. Selección de Soluciones Tecnológicas:**<br>• Investigación y selección de firewalls robustos que se ajusten a los requisitos de seguridad de la red.<br>• Implementación de sistemas de segmentación de red para limitar el movimiento lateral de posibles amenazas.<br>• Elección e implementación de sistemas de prevención de intrusiones (IPS) para la detección y respuesta proactiva ante intentos de ataques.<br>**4. Diseño de la Arquitectura de Seguridad de la** |

| **Nombre del proyecto** | **Protección de la red** |
|---|---|
| | **Red:**<br><br>• Desarrollo de un diseño de seguridad de red que incorpore las soluciones seleccionadas.<br>• Configuración de políticas y reglas en los dispositivos de seguridad de red.<br>• Planificación de la segmentación de red de acuerdo con las necesidades y requisitos de la entidad.<br>**5. Implementación Gradual:**<br><br>• Despliegue progresivo de las soluciones de seguridad en la red.<br>• Configuración de reglas y políticas de seguridad de manera coherente.<br>• Pruebas de funcionalidad y rendimiento de los dispositivos de seguridad.<br>**6. Monitoreo y Gestión Continua:**<br><br>• Implementación de herramientas de monitoreo de red para supervisar el tráfico y detectar posibles anomalías.<br>• Establecimiento de alertas para notificar sobre eventos de seguridad.<br>• Configuración de sistemas de registro para el análisis de eventos de seguridad.<br>**7. Capacitación del Personal:**<br><br>• Capacitación del personal en las nuevas políticas de seguridad y procedimientos.<br>• Concientización sobre las mejores prácticas de seguridad y el uso adecuado de la red.<br>**8. Evaluación de la Efectividad:**<br><br>• Realización de evaluaciones periódicas de la efectividad de las medidas de seguridad implementadas.<br>• Análisis de registros y eventos de seguridad para mejorar la respuesta a incidentes.<br>**9. Revisión y Mejora Continua:**<br><br>• Evaluación regular de la arquitectura de seguridad de red.<br>• Ajuste de políticas y configuraciones en función de las lecciones aprendidas y la evolución de las amenazas. |
| **Recursos** | Oficina de seguridad y privacidad de la información – Área de Tecnologías de la Información y de las Comunicaciones – TIC |
| **Fecha Inicio estimada** | 2024 |
| **Fecha Fin estimada** | 2026 |


## 12. ANEXOS

No aplica

## 13. CONTROL DE CAMBIOS

| No. | Fecha | Descripción del cambio o modificación |
|---|---|---|
| 1 | Enero 2024 | Primera emisión. Aprobado en Comité Institucional de Gestión y Desempeño (acta 05-2024) |

| | | |
|---|---|---|
| ALVARO IVAN TORRES GONZALEZ Firmado digitalmente por ALVARO IVAN TORRES GONZALEZ Fecha: 2024.01.31 08:04:36 -05'00' | Firmado digitalmente por MARICELA OYOLA MARTINEZ | RUBEN DARIO OCHOA ARBELAEZ Firmado digitalmente por RUBEN DARIO OCHOA ARBELAEZ |
| **ALVARO IVÁN TORRES GONZÁLEZ** | **MARICELA OYOLA MARTINEZ** | **RUBÉN DARÍO OCHOA ARBELÁEZ** |
| Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información | Subdirector Administrativo y Financiero | Director General |
| **ACTUALIZÓ** | **REVISÓ** | **APROBÓ** |