Contenido

LISTA DE VERSIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
0	11/08/2025	Se elimina el documento DI-OPL-004 Políticas Específicas de Seguridad de la Información dando lugar al Manual de Políticas de Seguridad de la Información incluyendo los siguientes puntos: Actualización de las referencias normativas y legales Ajuste en la redacción del alcance Se cambia el nombre de Políticas a Manual conforme los lineamientos d la Resolución 2277 de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) que actualiza el Anexo 1 de la Resolución 500 de 2021 Se ajusta estructura conforme la actualización de la política de seguridad y privacidad de la información basada en la ISO 27001-27002:2022 *Políticas Organizacionales * Política del Recurso Humano * Políticas de Control Físico * Políticas de Control Tecnológico

INTRODUCCIÓN

El presente documento se considera como una extensión de la POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, en la cual se plasman los compromisos de la alta dirección con el Subsistema de Gestión de Seguridad de la Información – SGSI en el Ministerio de las Culturas, las Artes y los Saberes (en adelante el "Ministerio" o la "Entidad"),

A continuación, se presentan las políticas específicas de seguridad y privacidad de la información, las cuales guiaran a los procesos y colaboradores en la implementación, cumplimiento y seguimiento de estas.

1. OBJETIVO GENERAL

Apoyar la implementación de los lineamientos establecidos en la Política General de Seguridad y Privacidad de la Información con el fin de proteger la información del acceso, uso y divulgación no autorizada, a través de la gestión que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Subsistema de Gestión de Seguridad de la información - SGSI del Ministerio.

1.1. OBJETIVOS ESPECÍFICOS

Definir lineamientos

Definir los lineamientos, documentos y procesos necesarios para la protección de la información.

Cumplimiento legal y normativo

Cumplir con las disipaciones legales y normatividad vigente referentes a la seguridad de la información y el tratamiento de los datos personales.

2. ALCANCE

Esta política aplica a todos los colaboradores del Ministerio. Es responsabilidad de ellos cumplir con todos los lineamientos establecidos en el Subsistema de Gestión de Seguridad de la Información (SGSI). Por lo tanto, es de obligatorio cumplimiento para los colaboradores del Ministerio y para los terceros que interactúen con él.

3. DEFINICIONES

Amenaza: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a colaboradores, procesos o entidades no autorizadas.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por un colaborador, proceso o entidad autorizada.

Dispositivo Móvil: Para efectos de este documento se hace referencia a computadores portátiles y tabletas personales o de propiedad del Ministerio.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información, inesperados o no deseados, que tiene probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

Integridad: Propiedad de exactitud y completitud.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones.

Malware: Abreviatura de *malicious software*, este término engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento de este.

No repudio: Capacidad para corroborar que es cierta la reivindicación de que ocurrió un evento o una acción y las entidades que lo originaron.

Parte interesada: Persona u organización que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de información: Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información.

Tercero: Persona natural o Jurídica delegada por el contratista o funcionario para cumplir labores o servicios contratados, que requiere acceder a los sistemas de información o servicios tecnológicos para desarrollar un proyecto, programa o actividad relacionada con la gestión del Ministerio.

Vulnerabilidad: Debilidad de un activo o de un control que puede ser explotad por una o más amenazas.

4. GESTIONES SGSI

4.1. Gestión De Activos

Orientar a los colaboradores del Ministerio en el levantamiento, clasificación y manejo de los activos de información que producen, almacenan, recolectan o custodian atendiendo las disposiciones normativas vigentes.

4.2. Gestión De Riesgos

Definir una metodología para gestionar los riesgos de seguridad de la información y riesgos digitales en el Ministerio, con el fin de asegurar que el Subsistema de Gestión de Seguridad de la Información – SGSI logre los resultados previstos, se prevengan o reduzcan efectos indeseados y se consideren oportunidades que permitan el mejoramiento continuo.

4.3. Gestión De Incidentes

El objetivo de este procedimiento es propender porque los eventos, incidentes de seguridad de la información y debilidades de seguridad de la información sean detectados, analizados, mitigados y tratados eficiente y eficazmente.

4.4. Gestión De Continuidad De La Operación

Definir las actividades que garanticen de manera eficiente la continuidad de la prestación de servicios, la operación de los sistemas de información y los procesos, frente a un incidente que afecte el desarrollo cotidiano de la entidad en sus diferentes sedes.

4.5. Protección De Datos Personales

Asegurar el adecuado tratamiento de los datos personales que se recolectan, almacenan, usan, circulan y suprimen en el ejercicio de las funciones propias del Ministerio, dando así cumplimiento de lo dispuesto en la Ley 1581 de 2012 y las demás normas concordantes.

4.6. Gestión De Cultura Y Apropiación

Fomentar una Cultura de Seguridad de la información en los colaboradores del Ministerio que permita generar conciencia de sus deberes y responsabilidades frente a los activos de información y el Subsistema de gestión de seguridad de la información SGSI.

5. POLÍTICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se presentan las políticas que deben aplicarse como parte integral de la implementación del Sistema de Seguridad de la Información y el cumplimiento de la Política General de Seguridad y Privacidad de la Información.

Estas políticas están basadas en la norma ISO 27001:2022, la cual establece un marco para gestionar la seguridad de la información a través de políticas específicas organizadas en cuatro dominios clave:

Estas políticas específicas garantizan una protección integral de la información, alineándose con los estándares internacionales y fortaleciendo la resiliencia organizacional frente a amenazas y vulnerabilidades.

5.1. Políticas Organizacionales

Política de estructura organizacional de seguridad de la información

- Establecimiento del SGSI: El Ministerio de Cultura, en cumplimiento de su compromiso con la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), establece un esquema de seguridad de la información que define y establece roles y responsabilidades involucrando las actividades de operación, gestión y administración de la seguridad de la información a través de su Política de Seguridad y Privacidad de la Información.

- Adopción de Estrategia de Seguridad Digital: A través de un acto administrativo de carácter general, se adoptará la estrategia de seguridad digital, identificando el alcance y los responsables de su implementación.

- Aprobación y Comunicación de Políticas: Las políticas que componen el SGSI deben ser aprobadas por la Alta Dirección, publicadas, comunicadas y reconocidas por los colaboradores y las partes interesadas. Las actualizaciones se realizarán a intervalos planificados o si ocurren cambios significativos.

Política de gestión de activos de Información

- Procedimiento Formal: Documentar un procedimiento formal para la gestión de activos de información.
- Identificación y Mantenimiento de Activos: Las áreas del Ministerio deben identificar y mantener actualizados los activos de información que tengan a su cargo.

- Responsabilidad de los Líderes de Área: Los activos de información serán responsabilidad de los líderes de cada área.
- Notificación de Novedades: Es responsabilidad de cada área informar las novedades que puedan afectar la integridad, disponibilidad o confidencialidad de los activos de información.
- Propiedad de los Activos: Los activos de información son propiedad del Ministerio; los colaboradores deben devolverlos al finalizar su contrato o acuerdo.
- Documentación de Activos Para Devolver: Identificar y documentar todos los activos que deben ser devueltos, como información física, hardware de autenticación, equipos y dispositivos tecnológicos.
- Clasificación de la información: Se debe desarrollar e implementar procedimientos, mecanismos o herramientas para el etiquetado de la información acorde con los niveles de clasificación definidos y adoptados, dichas etiquetas permiten reconocer fácilmente la importancia del activo.

Política de uso de los activos

- Directrices de Uso: Implementar directrices para lograr y mantener la protección adecuada y el uso de los activos de información mediante la asignación a los usuarios finales según sus roles y funciones.
- Uso Exclusivo para Actividades Contractuales: La asignación de los activos de información es para uso exclusivo del desarrollo de las actividades contractuales asignadas en el Ministerio.
- Compromiso de Uso Aceptable: Los usuarios deben comprometerse a dar buen uso a los recursos tecnológicos, conforme a las políticas definidas por el SGSI.
- Responsabilidad de los Colaboradores: Todos los colaboradores que usen los activos de información del Ministerio deben seguir las políticas establecidas para el uso aceptable de los activos de información.

  A continuación, se mencionan actos de mal uso, sin embargo, estos no se limitan a:
  - Los recursos no podrán ser utilizados, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, prácticas de juegos en línea, programas destructivos (virus), material político/religioso o cualquier otro uso que no esté vinculado con las labores institucionales.

- Monitoreo y Auditoría: Los activos de información estarán sujetos a monitoreo y auditoría según sea necesario

Política de uso de los recursos tecnológicos.

- Buen Uso de Activos de Información: Todos los colaboradores deben hacer buen uso de los activos de información a los cuales tienen acceso y que son propiedad del Ministerio.
- Mantenimiento de Equipos: Solo el personal autorizado puede manipular, destapar y actualizar los equipos de cómputo.
- Almacenamiento de Archivos: No se permite mantener archivos no institucionales en discos duros de estaciones cliente o discos virtuales de red.
- Conexiones Eléctricas: No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información.
- Informe de Pérdida o Daño: La pérdida o daño de elementos o recursos tecnológicos debe ser informada de inmediato.
- Traslado de Recursos Tecnológicos: El traslado de recursos tecnológicos se realizará a través de las áreas designadas y la configuración estará a cargo del área de TI.
- Incidentes de Seguridad: Todo incidente de seguridad debe ser reportado a la mayor brevedad posible.
- Administración de Software: La administración del software es responsabilidad exclusiva del área de TI.
- Apagado de Equipos: Los equipos deben quedar apagados cuando no se usen y no se requiera realizar actividades vía remota.
- Gestión de Cambios: Definir y documentar la gestión de cambios en las instalaciones de procesamiento de información y los sistemas de información.

Política de uso del correo electrónico

- Uso Institucional: El correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional.

- Iniciativa de Uso Aceptable del Papel: Optar por el uso del correo electrónico en lugar de documentos físicos, siempre que las disposiciones legales lo permitan.
- Legalidad de Mensajes de Datos: Los mensajes de correo están respaldados por la Ley 527 de 1999.
- Correos Masivos: No se permite el uso de correos masivos salvo a través de cuentas autorizadas.
- Mensajes Sospechosos: Todo mensaje sospechoso debe ser reportado como incidente de seguridad.
- Registro en Páginas No Institucionales: No se debe registrar el correo institucional en sitios no relacionados con fines institucionales.
- Transferencia de Contenidos: No se permite el uso del correo para la transferencia de contenidos ofensivos o no relacionados con los fines institucionales.
- Distribución de Información Reservada: No se debe usar el correo institucional para distribuir información reservada sin autorización previa.
- Leyenda de Confidencialidad: Los mensajes deben contener una leyenda de confidencialidad en la firma institucional.
- Servicio de Correo Autorizado: El único servicio de correo autorizado es el asignado por el área de TI, cumpliendo con todos los requerimientos técnicos y de seguridad.

Política de uso de internet

- Navegación Segura: Establecer lineamientos para garantizar la navegación segura y el uso adecuado de la red por parte de los usuarios.
- Permisos de Navegación: La Oficina de Tecnologías de la Información autorizará los cambios solicitados de permisos de navegación.
- Controles de Acceso: Implementar controles para evitar el acceso a contenidos ofensivos y restringir el acceso a sistemas de almacenamiento en la nube y cuentas de correo no institucional.
- Monitoreo de Accesos: El Ministerio se reserva el derecho de monitorear los accesos y el uso del servicio de internet.

Política para uso de dispositivos móviles

- Registro de Dispositivos: Todo dispositivo móvil que ingrese o se retire del Ministerio debe ser registrado, identificando como mínimo:
  - Fecha y hora de ingreso y salida.

- Identificación de la persona que lo ingresa o retira.
- Nombre(s) y Apellido(s) de la persona que lo ingresa o retira.
- Dependencia a la que pertenece o se dirige.
- Serial del dispositivo.
- Marca del dispositivo.

- Configuración y Seguridad: Los dispositivos móviles asignados deben mantener la configuración respectiva para restringir la instalación de software y tener mecanismos que impidan el robo o pérdida.
- Acceso a la Red: Los dispositivos móviles deben estar configurados para acceder mediante credenciales asignadas.
- Cifrado de Información: Los dispositivos móviles retirados de las instalaciones deben contener mecanismos de cifrado.
- Antivirus Institucional: Todos los dispositivos móviles asignados deben tener instalado el antivirus institucional.
- Conexión a la Red: La conexión a la red para dispositivos móviles ajenos al Ministerio debe estar segmentada para proveer únicamente el servicio de internet.
- La pérdida o robo de dispositivos móviles propiedad de la Entidad debe ser reportada:
  - Grupo de Gestión Administrativa y de Servicios.
  - Autoridades pertinentes

Política de uso de mensajería instantánea y redes sociales

- Protección de la Información: Definir pautas para asegurar una adecuada protección de la información en el uso de servicios de mensajería instantánea y redes sociales.
- Responsabilidad Personal: La información publicada en redes sociales personales no está bajo el alcance del SGSI y es responsabilidad del usuario.
- Autorización de Información Institucional: Toda información distribuida en redes sociales debe ser autorizada por los líderes de área.
- Uso del Nombre del Ministerio: No se debe utilizar el nombre del Ministerio para difamar o afectar la imagen de la entidad.
- Manejo y Gestión de Redes Sociales: Las personas designadas para el manejo de redes sociales deben acatar las directrices establecidas.
- Solicitud de Apertura de Redes Sociales: Las áreas que requieran la apertura de redes sociales deben presentar una solicitud motivada.
- Seguridad de Cuentas: Aplicar complejidad en las contraseñas y realizar cambios periódicos.

- Verificación de Medidas de Seguridad: El SGSI realizará verificaciones de las medidas de seguridad implementadas.
- No Vinculación de Correos Personales: No se deben vincular correos personales en redes sociales institucionales.
- Administración desde Dispositivos Personales: No se recomienda la administración de redes sociales institucionales desde dispositivos personales.

Política de clasificación de la información

- Categorías de Clasificación: Adoptar las categorías de INFORMACIÓN PÚBLICA, INFORMACIÓN PÚBLICA RESERVADA e INFORMACIÓN PÚBLICA CLASIFICADA.
- Clasificación de Activos: Clasificar todos los activos de información indiferentemente de su medio de almacenamiento.
- Etiquetado de Información: Desarrollar e implementar lineamientos para el etiquetado de la información.
- Intercambio de Información: Incluir la clasificación en información intercambiada con otras entidades.
- Sistemas de Información Sensibles: Implementar mecanismos para indicar la clasificación en sistemas de información sensibles o críticos.

Política para la transferencia de información

- Protección de Información Transferida: Proteger la información transferida al interior y exterior del Ministerio.
- Control de Transferencias de Archivos: La Oficina de Tecnologías de la Información controla el uso de sistemas de transferencia de archivos vía FTP.
- Cifrado de Información en Transferencias: Usar mecanismos que no permitan la fuga o interceptación de información, preferiblemente cifrando la información transferida.
- Acuerdos de Confidencialidad: Las transferencias de información deben estar amparadas por acuerdos interinstitucionales o de confidencialidad.

Política de control y gestión de acceso

- Gestión de Usuarios: La Oficina de Tecnologías de la Información establecerá lineamientos para la gestión de usuarios, incluyendo el uso de credenciales únicas.

- Registro Centralizado de Accesos: Mantener un registro centralizado de los accesos suministrados.
- Herramientas Autorizadas: Realizar accesos únicamente por las herramientas autorizadas, evitando el uso de software de acceso remoto no licenciado.
- Principio de Mínimo Privilegio: Aplicar el principio de mínimo privilegio necesario para la realización de actividades asignadas.
- Revisión de Usuarios Activos: Los administradores de los sistemas de información deben realizar revisiones periódicas de los usuarios activos.
- Notificación de Desvinculaciones: Los líderes de área deben notificar las desvinculaciones de funcionarios para que sean retirados los accesos.
- Configuración de Contratistas: Configurar automáticamente la inhabilitación de credenciales asignadas a contratistas al finalizar el contrato.
- Uso de Dispositivos de Almacenamiento Externo: El Ministerio se reserva el uso de dispositivos de almacenamiento externo, como dispositivos móviles, DVD, CD.

Política de establecimiento, uso y protección de claves de acceso

- Uso de Credenciales Propias: Ningún usuario debe acceder a la red o servicios del Ministerio utilizando credenciales de otro usuario.
- Responsabilidad de Acciones Realizadas: Toda acción realizada usando la clave de acceso es responsabilidad directa del usuario.
- Suministro de Claves: La Oficina de Tecnologías de la Información suministrará las claves para el acceso a los servicios autorizados.
- Solicitud de Cambio de Contraseña: El cambio de contraseña solo debe ser solicitado por el titular de la cuenta.
- Protección de Credenciales: Los colaboradores deben proteger sus credenciales y no dejarlas visibles.
- Política de Cambio de Contraseña: Implementar mecanismos para que los usuarios cambien su contraseña al usarla por primera vez y periódicamente.
- Requisitos de Seguridad de Contraseñas: Las contraseñas deben tener un mínimo de ocho caracteres, cambiarse cada 60 días y no repetir las últimas doce contraseñas.
- Doble factor de autenticación: Todos los servicios institucionales que consideren e incorporen opciones de doble factor de autenticación deben activarse con el fin de prevenir accesos no autorizados y fortalecer la seguridad de la información. Los colaboradores deben seguir los siguientes lineamientos para el uso del doble factor de autenticación:

- Implementación Obligatoria: La activación del doble factor de autenticación es obligatoria en todos los sistemas críticos y en aquellos que manejen información sensible.
- Métodos de Autenticación: Los métodos aceptables incluyen, pero no se limitan a, autenticación por aplicaciones móviles (como Google Authenticator o Microsoft Authenticator), mensajes SMS, correos electrónicos, y dispositivos físicos de autenticación (como llaves de seguridad).

Manejo de contraseñas para administradores de TI

- Ingreso con Credenciales de Directorio Activo: Garantizar que el ingreso a la administración se realice con credenciales de directorio activo.
- Desactivación de Contraseñas Predefinidas: Las contraseñas de cuentas predefinidas deben ser desactivadas o cambiadas tras la instalación del producto.
- Confidencialidad de Credenciales: Los administradores de TI no deben compartir sus credenciales sin autorización.
- Contraseñas de Alta Complejidad: Utilizar contraseñas de alta complejidad y servicios de autenticación según el rol asignado.

Política en la relación con proveedores

- Seguridad en el Acceso y Procesamiento: Mantener la seguridad de la información y servicios de procesamiento a los cuales tienen acceso terceras partes.
- Obligaciones Contractuales: Establecer obligaciones en los contratos con terceros que contemplen la gestión de seguridad de la información.
- Control de Relaciones Contractuales: Implementar mecanismos de control en las relaciones contractuales para asegurar el cumplimiento de las políticas de seguridad de la información.
- Acuerdo de Confidencialidad: Incluir una causal de terminación de contrato por incumplimiento de las políticas de seguridad.
- Supervisión de Contratos: Los supervisores de contratos deben realizar seguimiento y control de los servicios suministrados.
- Devolución de Activos: Los proveedores y contratistas deben devolver los activos de información asignados.
- Gestión de Cambios en Servicios: Establecer mecanismos para gestionar cambios en los servicios suministrados.

Política para el uso de servicios en la nube

- Gestión de Riesgos de Seguridad: Gestionar los riesgos de seguridad en el uso de servicios en la nube.
- Responsabilidad Compartida: Definir la responsabilidad compartida de la seguridad de la información entre el proveedor del servicio y el Ministerio.
- Notificación de Cambios Sustanciales: Exigir al proveedor de servicio que notifique antes de realizar cambios sustanciales que afecten al Ministerio.
- Tratamiento de Información: Validar los requisitos de confidencialidad, integridad y disponibilidad en los acuerdos de servicios.
- La entidad, en el marco de los servicios contratados en la nube, podrá incorporar componentes y/o herramientas basadas en inteligencia artificial, siempre que estas hayan sido previamente identificadas, evaluadas y aprobadas desde una perspectiva integral de gestión del riesgo. Estas herramientas podrán ser nativas del proveedor de servicios en la nube o integradas por la entidad en sus propios sistemas de información o aplicaciones, conforme a los lineamientos establecidos en materia de seguridad, privacidad y cumplimiento normativo.

Política de gestión de los incidentes de la seguridad de la información

- Comunicación de Incidentes: Garantizar que los eventos e incidentes de seguridad sean comunicados y atendidos oportunamente.
- Respondientes para la Atención de Incidentes: Establecer los responsables para la atención de incidentes dentro del Ministerio.
- Gestión de Evidencias: Asegurar una gestión consistente y eficaz de la evidencia relacionada con incidentes de seguridad.
- Mejora de Controles de Seguridad: Fortalecer los controles de seguridad a través de la documentación y conocimiento de los incidentes.

Política de seguridad de la información durante la interrupción

- Procedimientos y Estrategias de Continuidad: Definir procedimientos y estrategias para contrarrestar interrupciones y proteger los procesos críticos.
- Prevención de Interrupciones: Prevenir interrupciones en la plataforma informática que afecten los procesos críticos de TI.
- Planes de Continuidad de Proveedores: Asegurar que los proveedores de servicios TI críticos tengan planes de continuidad.

- Inclusión de Seguridad en Continuidad del Negocio: Incluir requisitos de seguridad en los procesos de gestión de la continuidad del negocio.
- Plan de Continuidad TI: Desarrollar e implementar un Plan de Continuidad TI para asegurar la restauración de los procesos misionales de TI.
  Se debe definir un equipo para la planeación y ejecución de las pruebas de redundancia tecnológica u operativa del Ministerio.
- Documentar: Se deben generar informes o reportes de las pruebas realizadas a los planes de continuidad. Estos informes deben incluir recomendaciones, lecciones aprendidas y acciones de mejora. Esta información debe estar disponible para los colaboradores interesados o que participaron en las pruebas

Política de cumplimiento de requisitos legales, estatutarios, reglamentarios y contractuales

- Gestión de Riesgos de Incumplimiento: Gestionar riesgos para prevenir el incumplimiento de obligaciones legales relacionadas con seguridad de la información.
- Protección de Datos Personales: Asegurar que los sistemas de información que capturen datos personales cumplan con la política de protección de datos personales.
- Identificación de Requisitos Legales: Identificar, documentar y actualizar los requisitos legales relacionados con seguridad de la información.
- Licenciamiento de Software: Garantizar que todo el software utilizado esté protegido por derechos de autor y licencias de uso.
- Cumplimiento de Leyes de Derechos de Autor: Los colaboradores deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software.

Política de tratamiento de datos personales

- Cumplimiento de la Ley 1581 de 2012: El tratamiento de datos personales se realizará conforme a la Ley 1581 de 2012 y sus decretos reglamentarios.
- Datos de Menores de Edad: El tratamiento de datos personales de menores de edad debe realizarse con autorización de los padres o representantes legales.
- Captura de datos: Todos los sistemas de información que capturen datos personales de los ciudadanos deben cumplir con la política y el manual de tratamiento y protección de datos personales definidos por el Ministerio.

- Avisos en Sedes: Fijar avisos en las sedes del Ministerio donde se realice recolección de datos personales y biométricos.
- Sesiones Virtuales: Informar a los asistentes sobre la grabación de sesiones virtuales y obtener su autorización.

Política de revisión independiente de la seguridad de la información.

- Garantizar el Funcionamiento del SGSI: Asegurar el funcionamiento del SGSI conforme a las políticas y procedimientos implementados.
- Verificación de Cumplimiento: La Oficina de Control Interno de Gestión realizará verificaciones de cumplimiento de objetivos, controles, políticas y procedimientos.
- Supervisión por Líderes de Proceso: Los líderes de proceso deben verificar el cumplimiento de las políticas de seguridad de la información en sus áreas.
- Revisiones Esporádicas: La Oficina de Tecnologías de la Información realizará revisiones esporádicas no programadas para verificar el cumplimiento de las políticas de seguridad.

Política de cumplimiento

- Obligatoriedad de Cumplimiento: Los colaboradores deben cumplir con todos los aspectos de esta política.
- Acciones Disciplinarias: En caso de infracción, el Ministerio tomará acciones disciplinarias y legales correspondientes.
- Prevención de Incumplimientos: Prevenir el incumplimiento de leyes, estatutos, regulaciones y obligaciones contractuales relacionadas con la seguridad de la información

5.2. Política de Seguridad del Recurso Humano

- Responsabilidades en Seguridad de la Información: Asegurar que todos los colaboradores adopten sus responsabilidades en relación con las políticas de seguridad de la información.
- Acuerdos Contractuales: Establecer la responsabilidad del colaborador en cuanto a seguridad de la información en los acuerdos contractuales.
- Conciencia sobre Seguridad de la Información: Establecer estrategias para que los colaboradores tomen conciencia sobre seguridad de la información.

- Procedimientos Disciplinarios: Articular procedimientos disciplinarios en situaciones de incumplimiento de las políticas de seguridad.
- Identificación de Novedades Contractuales: Implementar procedimientos para identificar novedades contractuales y retirar o modificar los accesos.

Política de trabajo a distancia

- Identificación de Necesidades de VPN: Identificar y licenciar la VPN para el trabajo a distancia.
- Uso de Herramientas Colaborativas: Usar herramientas colaborativas de Microsoft 365 para el envío, recepción, transferencia y almacenamiento de información.
- Acceso Remoto: Autorizar el uso de VPN para acceso remoto según las necesidades específicas del área solicitante.
- Seguridad en Equipos Personales: Recomendar la instalación y actualización de antivirus en equipos personales utilizados para VPN.
- Autenticación Multifactor: Configurar mecanismos de autenticación multifactor para fortalecer la seguridad.
- Configuraciones de Seguridad: La Oficina de Tecnologías de la Información realizará configuraciones de seguridad y revocación de acceso a la VPN.
- Monitoreo del Uso de Herramientas: Monitorear el uso de herramientas de Microsoft 365 para garantizar el cumplimiento de políticas y realizar revisiones periódicas de seguridad

Política de reporte de eventos de seguridad de la información

- Reporte de Eventos Sospechosos: Los colaboradores y terceros deben reportar cualquier evento sospechoso observado en los activos de información.
- Definición de Canales de Reporte: La Oficina de Tecnologías de la Información definirá y socializará los canales para el reporte de eventos de seguridad detectados.

5.3. Política de seguridad física

Política de perímetros y entrada física

- Sistema de Seguridad Física: Implementar un sistema de seguridad física para las instalaciones del Ministerio.

- Registro de Visitantes: Los visitantes deben registrarse y ser autorizados para ingresar, y estar acompañados durante su estancia.
- Alarmas de Intrusión: Implementar alarmas de detección de intrusos en centros de datos y centros de cableado.
- Perímetros de Seguridad: Definir y usar perímetros de seguridad para proteger áreas de procesamiento de información sensible o crítica.
- Controles de Acceso Físico: Los controles de acceso físico deben permitir el acceso solo a personal autorizado.
- Carné Visible: Todos los colaboradores deben portar el carné en lugar visible; los visitantes deben portar una escarapela.
- Inspección de Material de Carga: Inspeccionar el material que ingresa para detectar presencia de materiales peligrosos.
- Restringir Acceso a Áreas Críticas: Implementar restricciones de acceso a áreas de despacho y carga.

Política de escritorio despejado y pantalla limpia

- Conservación de Escritorio Libre: Mantener el escritorio libre de información que pueda ser alcanzada o utilizada por terceros no autorizados.
- Cierre de Sesión Automático: Configurar los equipos con cierre de sesión automático.
- Bloqueo de Pantalla: Los usuarios deben bloquear la pantalla de su computador cuando no estén en su puesto de trabajo.
- Cierre de Aplicaciones: Cerrar las aplicaciones y servicios de red cuando no sean necesarios.
- Retiro de Documentos Impresos: Retirar inmediatamente los documentos impresos con información reservada y no dejarlos en el escritorio sin custodia.

Política de protección contra amenazas físicas y ambientales

- Protección de Infraestructura de Soporte: Asegurar la protección de la infraestructura de soporte y las redes.
- Prohibiciones en Centros de Datos: No fumar, introducir alimentos o bebidas, portar armas o mover equipos sin autorización en centros de datos.
- Registro de Accesos a Áreas Críticas: Mantener herramientas que registren el acceso a áreas críticas.
- Controles contra Amenazas: Implementar controles contra incendios, inundaciones y sobretensiones eléctricas.

- Protección de Medios y Equipos: Mantener medios y equipos con medidas de protección físicas y lógicas.

Política de medios de almacenamiento

- Riesgos de Medios Extraíbles: Gestionar los riesgos de medios de almacenamiento extraíbles, restringiendo su uso.
- Medios de Almacenamiento Autorizados: Usar únicamente medios de almacenamiento autorizados.
- Monitoreo de Transferencias: Monitorear la transferencia de información cuando se utilicen medios de almacenamiento extraíbles.
- Procedimiento de Transferencia de Medios Físicos: Implementar un procedimiento para la transferencia de medios físicos.

Política de seguridad del cableado

- Protección de Líneas Eléctricas y de Telecomunicaciones: Implementar controles para proteger las líneas eléctricas y de telecomunicaciones.
- Separación de Cables: Mantener separados los cables de alimentación y comunicación.
- Conductos Blindados y Alarmas: Usar conductos blindados, cajas cerradas y alarmas en puntos de terminación.
- Acceso Controlado a Paneles: Establecer mecanismos de acceso controlado a paneles de conexión y centros de cableado.

Política de mantenimiento de equipos

- Cronograma de Mantenimiento: Establecer un cronograma para el mantenimiento de equipos tecnológicos.
- Personas Autorizadas: Solo personas autorizadas realizarán reparaciones y mantenimientos.
- Ficha Técnica de Mantenimiento: Documentar cada mantenimiento con una ficha técnica.
- Mantenimiento Remoto: Solicitar autorización para mantenimiento remoto a través de un mecanismo seguro.

Política de eliminación segura o reutilización de equipos

- Eliminación de Información No Necesaria: Eliminar de forma permanente la información no necesaria en equipos de salas de reuniones.

- Borrado Seguro: Borrar de manera segura la información en medios de almacenamiento reusable.
- Cifrado de Información Confidencial: Cifrar la información confidencial en medios removibles.
- Eliminación de Medios Físicos: Disponer de medios físicos de forma segura mediante incineración, destrucción o borrado seguro.

5.4. Política de las operaciones TIC

Política de dispositivos tecnológicos y redundancias

- Actividades Operacionales: Definir y documentar actividades operacionales como copias de respaldo y manejo de errores.
- Seguimiento de Recursos: Realizar seguimiento al uso de recursos y proyecciones de capacidad futura.
- Monitoreo de Servicios y Dispositivos: Monitorear los servicios y dispositivos tecnológicos.
- Instalación de Software Externo: No instalar software externo sin aprobación.
- Controles contra Código Malicioso: Implementar controles contra código malicioso.
- Asignación de Dispositivos: Realizar la asignación de dispositivos tecnológicos con configuraciones de seguridad.
- Licenciamiento de Software: Licenciar software de protección contra código malicioso y mantener actualizados los sistemas de procesamiento de información.
- Redundancias en Servicios Críticos: Implementar redundancias en servicios tecnológicos críticos.

Política de accesos con privilegios.

- Control de Accesos con Privilegios: Controlar la asignación de accesos con privilegios a través de un proceso.
- Solicitudes y Aprobaciones: Las solicitudes de accesos con privilegios deben ser aprobadas por el responsable del activo de información.
- Límite de Tiempo: Limitar los accesos con privilegios a un rango de tiempo específico.
- Revisión Regular: Revisar regularmente los accesos con privilegios otorgados.

- Uso Exclusivo para Tareas Administrativas: Los accesos con privilegios deben ser usados solo para tareas administrativas.

Política de acceso a sistemas y aplicaciones

- Restricción de Accesos: Restringir el acceso a la información y funcionalidades de las aplicaciones según los niveles de autorización.
- Monitoreo y Auditoría: Mantener sistemas y aplicaciones monitoreados y auditados.
- Credenciales Diferenciadas: Diferenciar las credenciales de acceso para ambientes de pruebas y producción.
- Control de Acceso a Códigos Fuente: Controlar el acceso a códigos fuente y mantener un registro de auditoría.
- Seguridad en Autenticación: Implementar mecanismos de seguridad en la autenticación de usuarios.

Política de gestión de vulnerabilidades

- Monitoreo de Vulnerabilidades Técnicas: Definir estrategias de monitoreo de vulnerabilidades técnicas.
- Notificación y Plan de Remediación: Exigir a proveedores notificación y plan de remediación de vulnerabilidades.
- Pruebas de Vulnerabilidades: Realizar pruebas planificadas y documentadas para evaluar vulnerabilidades.
- Evaluación de Riesgos: Validar riesgos del despliegue de actualizaciones de firmware o sistemas operativos antes de su instalación.

Política de controles criptográficos

- Protección de Activos de Información: Implementar controles criptográficos para proteger activos de información reservados.
- Ciclo de Vida de Llaves Criptográficas: Definir el ciclo de vida de llaves criptográficas.
- Cifrado de Información en Medios de Almacenamiento: Usar herramientas de cifrado para la información en medios de almacenamiento.
- Cifrado en Portátiles: Instalar y configurar herramientas de cifrado en los portátiles del Ministerio.

Política de respaldo y restauración de información

- Medios de Respaldo Adecuados: Proporcionar medios de respaldo para asegurar la recuperación de información esencial y software.
- Verificación de Copias de Seguridad: Verificar la correcta ejecución de las copias de seguridad.
- Pruebas de Restauración: Realizar tareas de restauración aleatorias y documentarlas.
- Responsabilidad de Almacenamiento: Los colaboradores deben almacenar la información en los medios dispuestos para respaldos.
- No Realizar Copias en Medios Extraíbles: No realizar copias de información en medios extraíbles.
- Custodia de Copias Idénticas: Mantener copias idénticas de sistemas operativos para contingencias.

Política de seguridad de las comunicaciones

- Control de Redes y Sistemas de Comunicaciones: Implementar mecanismos de control para mantener la disponibilidad de redes de datos y sistemas de comunicaciones.
- Segmentación de Servicios: Segmentar los servicios de información, usuarios y sistemas.
- Autenticación en Servicios de Red: Proteger servicios de red con medios de autenticación.
- Conexión Segura a Servicios de Red: Implementar mecanismos técnicos para la conexión segura a servicios de red.
- Zona DMZ: Disponer de una zona DMZ para limitar conexiones desde la red interna hacia Internet y viceversa.
- Internet para Visitantes: Proveer servicio de internet para visitantes del Ministerio.

Política de registro y seguimiento de eventos de sistemas de información y comunicaciones

- Metodología de Revisión y Escritura de Eventos: Documentar una metodología de revisión y escritura de eventos que permita identificar actividades por usuario, excepciones, fallas y eventos de seguridad.
- Sincronización de Relojes: Mantener los relojes de todos los dispositivos tecnológicos sincronizados con una única fuente de referencia.

Política de adquisición, desarrollo y mantenimiento de sistemas de información

- Seguridad en el Ciclo de Vida de Sistemas de Información: Garantizar que la seguridad es parte integral del ciclo de vida de los sistemas de información.
- Control de Instalación y Cambios: Documentar lineamientos para el control de instalación y cambios de sistemas.
- Requisitos de Seguridad en Adquisición y Desarrollo: Definir y documentar requisitos de seguridad para la adquisición y desarrollo de sistemas.
- Separación de Entornos: Garantizar la separación de entornos de desarrollo, pruebas y producción.
- Auditoría de Sistemas de Información: Aplicar mecanismos de auditoría a todos los sistemas de información.
- Software Libre: Las solicitudes para uso de software libre deben ser avaladas por el oficial de seguridad.
- Desarrollo por Terceros: Asegurar que el desarrollo de sistemas por terceros cumpla con los estándares y políticas de seguridad.
- Enmascaramiento de Datos en Pruebas: Usar mecanismos de enmascaramiento o sustitución de datos en pruebas que involucren información sensible.

Política de protección de la información durante auditorias

- Acceso a Sistemas para Auditorías: Especificar el sistema que requiere acceso durante las auditorías.
- Modo Lectura: Otorgar acceso en modo lectura, salvo que se requiera de otra forma.
- Copias Aisladas para Pruebas: Realizar pruebas en copias aisladas del sistema con parámetros de seguridad.
- Disponibilidad de Pruebas: Realizar pruebas fuera del horario laboral si afectan la disponibilidad.

6. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad (Statement of Applicability - SOA) es un documento que lista los controles que se implementarán en el Ministerio, así como las justificaciones de aquellos controles que no serán implementados. Este análisis se realiza evaluando el cumplimiento de la norma ISO 27002:2022 para cada uno de los controles establecidos en los dominios relacionados con la gestión de la seguridad de la información especificados en el estándar.

7. REFERENCIAS LEGALES Y NORMATIVAS

- Resolución 2277 de 2025: Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
- Decreto 767 de 2022: Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Resolución 746 de 2022: Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021

- Directiva Presidencial No. 02 de 2022: Reiteración de la Política pública en materia de seguridad digital

- Resolución 500 del 10 de marzo de 2021 del Ministerio de Tecnologías de la Información y Comunicaciones.

- ISO/IEC 27001:2022

- ISO/IEC 27002:2022

- Ley 1273 de 2009 Protección de la información y los datos (información como bien jurídico)

- Ley 1712 de 2014 Transparencia y acceso a la información
    - Decreto 103 de 2015 Reglamenta la ley 1712 de 2014
    - Resolución 3564 reglamenta los aspectos relacionados con la ley 1712

- Ley 1581 de 2012 Protección de datos personales
    - Decreto 1377 de 2013 Reglamenta parcialmente la Ley 1581 de 2012

- Decreto 1499 de 2017 Actualiza el Modelo Integrado de Planeación y Gestión – MIPG

- Decreto 1008 de 2018 Lineamientos generales de la política de gobierno digital

- DUR 1078 de 2015 Decreta la estructura del sector de tecnologías de la información y las comunicaciones

- CONPES 3854 de 2017 Política nacional de seguridad digital
- CONPES 3701 de 2015 Lineamientos de políticas para ciberseguridad y ciberdefensa