ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA RECREACION Y DEPORTE
Instituto Distrital de las Artes

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GTI-POL-02

V.7

20/06/2025

Instituto Distrital de las Artes -IDARTES-
Carrera 8 No. 15 - 46 - Bogotá
+57 (601) 379 5750
Código postal: 111711

BOGOTÁ

TABLA DE CONTENIDO

TABLAS

1. INTRODUCCIÓN

El Instituto Distrital de las Artes – IDARTES, en cumplimiento de su compromiso con la protección de la información y la transparencia institucional, ha adoptado un enfoque integral de seguridad y privacidad de la información. Para ello, implementa un Sistema de Gestión de Seguridad de la Información (SGSI), alineado con los marcos legales y técnicos vigentes, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de sus activos de información.

Es fundamental resaltar el compromiso institucional y la aprobación del Comité Institucional de Gestión y Desempeño en la implementación y seguimiento de la Política de Seguridad de la Información. Este compromiso garantiza la adopción de lineamientos estratégicos, el cumplimiento de las disposiciones legales vigentes y el fortalecimiento de la cultura organizacional en torno a la protección de los activos de información del IDARTES,

La política digital, seguridad y privacidad de la información aplica a todos los funcionarios, contratistas, proveedores y demás usuarios de los servicios informáticos de la Entidad, quienes deben conocer y cumplir con las normas establecidas. Su desconocimiento no exime de responsabilidad ante incidentes de seguridad. Esta política se desarrolla en el marco de las disposiciones del Gobierno Digital, como el Decreto 767 de 2022 y la Resolución 500 de 2021 del MinTIC, que orientan la gestión de riesgos, el manejo de incidentes y la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). La planificación e implementación de esta política es transversal a los procesos institucionales, respondiendo a las necesidades del IDARTES y alineándose con su misión, visión y estructura, como parte de su compromiso con una gestión pública segura, responsable y transparente.

2. OBJETIVO GENERAL

Establecer lineamientos necesarios, con el fin de fortalecer la gestión de seguridad y privacidad de la Información del IDARTES, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información-SGSI, basado en la identificación, valoración y gestión de los riesgos asociados a ella; propendiendo por la protección de su confidencialidad, integridad, disponibilidad y privacidad de la información.

2.1 Objetivos Específicos

- Establecer las políticas de seguridad de la información necesarias para la protección de los activos de información, las cuales se desarrollan alineadas con el Modelo de Seguridad y Privacidad de la Información - MSPI, el anexo A de la norma ISO/IEC 27001:2013, así como el cumplimiento de los requisitos legales, contractuales y normativos aplicables a la Entidad.
- Implementar y mejorar continuamente el MSPI como mecanismo para brindar a los ciudadanos y colaboradores confianza digital en torno al uso y gestión de los datos, al cumplimiento legal y mantener una actitud ética, transparente y en concordancia con la visión y misión de la Entidad.

- Integrar la seguridad de la información con la estrategia misional para apoyar los objetivos de la entidad, gestionar los riesgos y fortalecer la seguridad en sus componentes de integridad, disponibilidad y confidencialidad.
- Gestionar de manera eficaz los riesgos en la seguridad y privacidad de la información identificados por el IDARTES.
- Sensibilizar sobre los diferentes temas relacionados con seguridad digital y privacidad de la información hacia los colaboradores, contratistas y demás partes interesadas del IDARTES.

3. ALCANCE Y APLICABILIDAD

Esta política es de obligatoria implementación para servidores públicos, contratistas y terceros del Instituto Distrital de las Artes – IDARTES, la Política pretende asegurar los componentes de la información como son: la confidencialidad, integridad, disponibilidad y privacidad bajo un enfoque de mejora continua y autocontrol en los procesos y en la prestación de los servicios, con base en la sensibilización de cada uno de los servidores del Instituto Distrital de las Artes – IDARTES y el apoyo del equipo de la Oficina Asesora de Planeación y Tecnologías de la Información-OAPTI, de manera que el acceso a la información oportuna y confiable facilite el ejercicio efectivo de los derechos constitucionales y legales, además de los controles ciudadano, político, fiscal, disciplinario y de gestión o administrativo, sin perjuicio de la reservas legales, es importante indicar que la aplicación e implementación de algunos controles se realizará de manera progresiva acorde a las capacidades y recursos asignados al proceso de TI.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento con la presente política, y el incumplimiento a la misma traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a la seguridad digital y privacidad de la información se refiere.

4. RESPONSABLES

Una responsabilidad vital del liderazgo es establecer y documentar una Política Digital, Seguridad y Privacidad de la Información que esté alineada con los objetivos estratégicos del Instituto, con el fin de que estén alineados con el contexto del Instituto y los requisitos de las partes interesadas.

También debe incluir un compromiso para:

- Cumplir requisitos aplicables relacionados con la seguridad de la información, tales como requisitos legales, expectativas de la ciudadanía y compromisos contractuales.
- La mejora continua de su SGSI, esta política digital, seguridad y privacidad de la información puede referirse o incluir controles que cubran los controles clave del SGSI de la entidad.

4.1 Compromiso de la Dirección General

La Dirección General debe brindar evidencia de su compromiso con la formulación, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar la información en el Instituto:

- A través de un Comité Institucional de Gestión y Desempeño del Instituto Distrital de las Artes - IDARTES es la responsable de la aprobación y de realizar el seguimiento a la estrategia de la implementación de la Política Digital, Seguridad y Privacidad de la Información.
- Debe comunicar a la entidad la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y las necesidades de la mejora continua conforme a los objetivos estratégicos del Instituto.

El director, subdirectores, gerentes, jefes de oficinas asesoras tiene la responsabilidad de hacer cumplir las normas y políticas de seguridad de la información establecidas por la Dirección General del Instituto Distrital de las Artes – IDARTES.

4.2 Compromiso de la Oficina Asesora de Planeación y Tecnologías de la Información

La Oficina Asesora de Planeación y Tecnologías de la Información es la responsable de la elaboración y/o modificación y/o actualización y/o eliminación e implementación, monitoreo y seguimiento de la Política Digita, Seguridad y Privacidad de la Información, asegurando los recursos adecuados y promoviendo así una cultura activa de seguridad en el Instituto.

- Establecer, mantener, actualizar, gestionar y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política digital, seguridad y privacidad de la información y todos sus capítulos, el uso de los servicios tecnológicos en todo el Instituto de acuerdo con las mejores prácticas y lineamientos de la Dirección General del Instituto Distrital de las Artes – IDARTES y directrices del Gobierno Nacional y Distrital.
- La Oficina Asesora de Planeación y Tecnologías de la Información lidera la definición de parámetros para el establecimiento de hardware, software y comunicaciones, así como de la arquitectura tecnológica. Sin embargo, la administración de la información en la fase de registro tanto en aplicativos como bases de datos es responsabilidad de cada área del IDARTES, con el fin de evitar modificación no autorizada o intencional o el uso indebido de los activos de información.
- Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Institución.
- Informar de los eventos que afecten la seguridad y privacidad de la información y de la infraestructura tecnológica del Instituto a las partes interesadas del IDARTES.
- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital del Instituto.
- Implementar y velar por el cumplimiento de la Política digital, seguridad y privacidad de la Información y sus componentes.
- Administrar los controles y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio del Instituto Distrital de las Artes – IDARTES.

- Analizar, aplicar y mantener los controles de seguridad implementados para actualizar, gestionar y mantener los datos e información gestionados en el Instituto.

4.3 Compromiso Comité Institucional de Gestión y Desempeño

- Desarrollar y actualizar la metodología para el análisis y gestión de riesgos de seguridad y para la clasificación de la información, según lo considere pertinente.
- Verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.
- El director, subdirectores, gerentes y jefes de oficinas asesoras tiene la responsabilidad de cumplir y hacer cumplir las normas y políticas de seguridad de la información establecidas por la Dirección General del Instituto Distrital de las Artes – IDARTES.

4.4 Compromiso del proceso de Tecnologías de la Información

- Garantizar la disponibilidad de los servicios y así mismo programar o informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de estos; así como gestionar su acceso de acuerdo con las solicitudes recibidas de las diferentes oficinas y subdirecciones siguiendo el procedimiento establecido.
- Establecer, mantener y divulgar las políticas y procedimientos de los servicios de tecnología, incluidos todos los capítulos que hacen parte de esta Política, en todo el Instituto de acuerdo con las mejores prácticas y directrices del Instituto y del Gobierno.
- Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información con miras a un gobierno de tecnologías consolidado.
- Brindar el soporte necesario a los usuarios a través de los canales de la mesa de ayuda actualmente implementados en la entidad.

4.5 Responsabilidades de los propietarios de la información

- Son propietarios de la información cada uno de los líderes de las Unidades de Gestión donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.
- Valorar y clasificar la información que está bajo su administración y/o generación.
- Autorizar, restringir y delimitar a los demás usuarios de la entidad el acceso a la información de acuerdo con los roles y responsabilidades de los diferentes funcionarios, contratistas o terceros que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.

- Determinar los tiempos de retención de la información en conjunto con él grupo de Gestión Documental y las áreas que se encarguen de su protección y almacenamiento de acuerdo con las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes.
- Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de esta.
- Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas y terceros en las diferentes dependencias de la entidad.

4.6 Responsabilidades de los funcionarios, contratistas y terceros usuarios de la información

- Los (as) funcionarios(as), contratistas y terceros que realicen labores en o para el Instituto Distrital de las Artes – IDARTES tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.
- Los usuarios de los sistemas y aplicativos deberán reportar a la Oficina Asesora de Planeación y Tecnologías de la Información las inconsistencias, anomalías y nuevos requerimientos sobre la plataforma tecnológica.
- Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones o Contrato.
- Manejar la Información de la entidad y rendir cuentas por el uso y protección de tal información, mientras esté bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
- Proteger la información a la cual acceden y procesan, para evitar su pérdida, alteración, destrucción o uso indebido.
- Evitar la divulgación no autorizada o el uso indebido de la información.
- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de esta.
- Informar a sus superiores y a la Oficina Asesora de Planeación y Tecnologías de la Información sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
- Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación y/o acceso no autorizado.
- Reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique dentro del IDARTES.
- Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos designados para el desarrollo de sus funciones.

- Usar únicamente el software autorizado que haya sido adquirido legalmente por la entidad. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de sus superiores y visto bueno de la Oficina Asesora de Planeación y Tecnologías de la Información.
- Divulgar, aplicar y el cumplir con la presente Política Digital, Seguridad y Privacidad de la Información.
- Aceptar y reconocer que, en cualquier momento y sin necesidad de previo aviso, la Dirección General y Control Interno del Instituto puede solicitar la inspección de la información bajo su responsabilidad, sin importar su ubicación o medio de almacenamiento. Esta revisión podrá incluir datos y archivos almacenados en correos electrónicos institucionales, sitios web y redes sociales oficiales, así como en unidades de red, computadores, servidores u otros dispositivos de almacenamiento pertenecientes a la entidad. Dichas inspecciones se realizarán con el propósito de verificar el cumplimiento de las políticas internas, apoyar procesos de auditoría y control, o dar respuesta a requerimientos de organismos de vigilancia, control o autoridades legales competentes.

Nota: En concordancia con la Ley 1581 de 2012 sobre protección de datos personales, el régimen general de habeas data, y la jurisprudencia constitucional vigente, se aclara que la inspección de la información institucional no vulnera el derecho a la intimidad ni a la protección de datos personales, en la medida en que se refiere a información de carácter institucional**,** contenida en activos, medios o plataformas propiedad del Instituto Distrital de las Artes – IDARTES. Esta inspección se hará respetando el principio de finalidad, proporcionalidad y legalidad, y no incluye la revisión de datos personales de carácter íntimo o privado no relacionados con el cumplimiento de funciones institucionales.

- Proteger y resguardar su información personal que no esté relacionada con sus funciones en la entidad.
- El Instituto Distrital de las Artes – IDARTES no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito.

4.7 Gestión de la Política Digital, Seguridad y Privacidad de la Información

Se busca brindar apoyo y orientación a la Dirección General con respecto a la seguridad y privacidad de la información, de acuerdo con los requisitos, los reglamentos y las leyes pertinentes.

4.7.1 Documento de la Política Digital, Seguridad y Privacidad de la Información

La Dirección General debe aprobar un documento de política digital, seguridad y privacidad de la información y lo debe publicar y comunicar a todos los servidores y partes externas pertinentes.

4.7.2 Revisión de la Política Digital, Seguridad y Privacidad de la Información

El documento de la Política Digital, Seguridad y Privacidad de la Información se debe revisar cuando se producen cambios significativos que así lo ameriten, para garantizar que sigue siendo adecuada, suficiente y eficaz.

4.8 Organización interna

El IDARTES establece la Política Digital, Seguridad y Privacidad de la Información y demás documentos relacionados con el Modelo de Seguridad y Privacidad de la Información, donde se definen roles y responsabilidades para la administración, operación y gestión de la Seguridad de la Información.

4.8.1 Compromiso de la dirección con la seguridad y privacidad de la información

La Dirección General debe apoyar activamente la seguridad dentro de la entidad con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad y privacidad de la información.

4.8.2 Coordinación de la seguridad y privacidad de la información

Las actividades de la seguridad y privacidad de la información deben ser coordinadas por los representantes de todas las partes de la entidad con roles y funciones laborales pertinentes.

4.8.3 Acuerdos sobre confidencialidad

Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades de la entidad para la protección de la información.

5. NORMATIVIDAD

Conforme a la norma ISO/IEC 27001, se consideran las referencias normativas que contienen información relevante para evaluar el cumplimiento del Instituto Distrital de las Artes (IDARTES) con los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI). En este sentido, se tendrá en cuenta la normativa vigente, la cual se encuentra consolidada y actualizada anualmente en el ***Normograma Institucional***, documento oficial que recopila el marco jurídico aplicable a la Entidad.

6. TÉRMINOS Y DEFINICIONES

- **Activo**: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.
- **Activo crítico**: Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectarán el cumplimiento de los objetivos estratégicos del IDARTES.
- **Administración de Riesgos**: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
- **Análisis de Impacto al Negocio (BIA)**: Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.
- **Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Alta Dirección**: Persona o grupo de personas que dirigen y controlan al más alto nivel de la entidad (Director, Subdirectores, Gerentes y Jefes de Oficina).
- **Centro de cableado**: El centro de cableado es el lugar donde se ubican los recursos de comunicación de tecnologías de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).
- **Cifrado:** Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
- **Control**: Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Confiabilidad de la Información**: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad**: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Código malicioso**: Es un código informático que crea brechas de seguridad para dañar un sistema informático.
- **Custodio**: Es una parte designada de la entidad, un cargo o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado".
- **Dato personal**: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. Debe entonces entenderse el "dato personal" como una información relacionada con una persona natural (persona individualmente considerada).
- **Dato personal público**: Toda información personal que es de conocimiento libre y abierto para el público en general.
- **Dato personal privado**: Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general.
- **Dato semiprivado**: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general.
- **Datos sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen

racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- **Datacenter**: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.
- **Disponibilidad**: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos
- relacionados con la misma, toda vez que lo requieran.
- **Dispositivos móviles**: Equipo celular smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.
- **Evento**: Es el suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política digital, seguridad y privacidad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
- **Evento de seguridad de la información**: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política digital, seguridad y privacidad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Home Office**: Oficina en casa o trabajo en casa.
- **Incidente de Seguridad**: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Integridad**: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Impacto**: Resultado de un incidente de seguridad de la información.
- **Legalidad**: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad
- **Mesa de Servicios**: Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que la Oficina de Tecnologías y sistemas de la Información recolecta las necesidades que tienen las dependencias en cuanto a los recursos tecnológicos.
- **No repudio**: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.
- **Partes interesadas**: Persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de Continuidad de Negocio**: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.
- **Privacidad de la información**: El derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Propietario de la información (titular)**: Es la unidad organizacional o proceso donde se crean los activos de información.
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso del IDARTES.
- **Seguridad Física**: Consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas ante amenazas a los recursos y la información confidencial, se refiere, a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.
- **Seguridad Lógica**: Medidas establecidas por la administración de usuarios y administradores de recursos de tecnología de información para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando los recursos tecnológicos y medios de información.
- **Servicios de almacenamiento de archivos "On line"**: Un servicio de alojamiento de archivos, servicio de almacenamiento de archivos online, o centro de medios online es un servicio de alojamiento de Internet diseñado específicamente para alojar contenido estático, mayormente archivos grandes que no son páginas web.
- **SGSI - Sistema de Gestión de Seguridad de la Información**: Consiste en un conjunto de políticas, procedimientos, directrices y recursos y actividades asociados, que son gestionados de manera colectiva por una organización con el fin de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio.
- **Shareware**: Clase de software o programa, cuyo propósito es evaluar por un determinado lapso, o con unas funciones básicas permitidas. para adquirir el software de manera completa es necesario un pago económico.
- **Software de Dominio Público**: es un software libre que no tiene un propietario, por ende, no existen derechos de autor, licencias o restricciones de distribución. Por este concepto, el software de dominio público se diferencia de un freeware, el cual conserva los derechos de autor.
- **Spam**: Es la denominación del correo electrónico no solicitado que recibe una persona. Dichos mensajes, también llamados correo no deseado o correo basura, suelen ser publicidades de toda clase de productos y servicios.
- **Software de Monitoreo**: Herramienta que constantemente vigila los dispositivos de una red de datos para informar a los administradores de redes mediante correo electrónico y/o alarmas el estado de estos.
- **Tipos de información**: cualquier tipo de información producida y/o recibida por las entidades públicas, sus dependencias y servidores públicos, y en general por cualquier persona que desarrolle actividades inherentes a la función de dicha entidad o que hayan sido delegados por esta, independientemente del soporte y medio de registro (análogo o digital) en que se produzcan, y que se conservan en:

    - Documentos de Archivo (físicos y electrónicos).
    - Archivos institucionales (físicos y electrónicos).
    - Sistemas de Información Corporativos.
    - Sistemas de Trabajo Colaborativo.
    - Sistemas de Administración de Documentos.
    - Sistemas de Mensajería Electrónica.

    - Portales, Intranet y Extranet.
    - Sistemas de Bases de Datos.
    - Discos duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), entre otros.
    - Cintas y medios de soporte (back up o contingencia).
    - Uso de tecnologías en la nube.

- **Terceros**: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.
- **Test de penetración**: Es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.
- **Topología de Red**: Se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados".
- **VIP**: Very important person.
- **VPN**: Red virtual privada por sus siglas en ingles Virtual Private Network.
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

7. CONDICIONES GENERALES

7.1 Evaluación de riesgos

La evaluación de riesgos es el núcleo de cualquier SGSI eficaz, incluso IDARTES con recursos no puede descartar la posibilidad de sufrir un incidente de seguridad de la información, por esto, la evaluación de riesgos es esencial para:

- Aumentar la probabilidad de identificar riesgos potenciales mediante la participación de personal que utiliza técnicas de evaluación sistemática
- Asignar recursos para abordar las áreas de mayor prioridad
- Tomar decisiones estratégicas sobre cómo gestionar los riesgos de seguridad de la información significativos y lograr así sus objetivos.

Así mismo, para definir los controles se tuvo en cuenta el documento *Plan de tratamiento de riesgos de seguridad y privacidad de la información y la matriz de riesgos de seguridad de la información,* que a su vez enmarca la gestión de activos de información que el IDARTES tiene definida.

7.2 Competencia

La implementación de controles efectivos de seguridad de la información depende del conocimiento y las habilidades de los empleados, proveedores y contratistas del IDARTES, para asegurar una base adecuada de conocimientos y habilidades, y se debe:

- Definir qué conocimientos y habilidades se requieren

- Determinar quién necesita del conocimiento y habilidades

7.3 Concienciación

Además de garantizar la competencia del personal clave en relación con la seguridad de la información, los empleados, proveedores y contratistas del IDARTES deberán conocer los elementos del SGSI, esto es fundamental para establecer una cultura de soporte dentro de la entidad. Todos los empleados, proveedores y contratistas deben tener en cuenta lo siguiente:

- La existencia de un SGSI a través del Modelo de Seguridad y Privacidad de la Información-MSPI y su razón de ser.
- Que tiene una política digital, seguridad y privacidad de la información y cuáles son sus elementos relevantes.
- Cómo pueden contribuir a que la entidad proteja la información y lo que deben hacer para ayudar a la organización a lograr sus objetivos de seguridad de la información.
- Qué políticas, procedimientos y controles son relevantes para ellos y cuáles son las consecuencias de no cumplirlos.

7.4 Comunicación

Para permitir que los procesos en el SGSI funcionen de manera efectiva, se debe asegurar actividades de comunicación planificadas y gestionadas que determinen

- Lo que necesita ser comunicado
- Cuando necesita ser comunicado
- A quién necesita ser comunicado
- Quién es responsable de la comunicación
- Cuáles son los procesos de comunicación.

7.5 Partes Interesadas

Las partes interesadas corresponden a las personas naturales o jurídicas con la cual el IDARTES interactúa en el ejercicio de sus funciones, que pueden afectar o ser afectadas por la Seguridad de la Información y en algunos casos, pueden manifestar un interés directo, explícito y comprometido con los objetivos y propósitos del Sistema de Gestión de Seguridad de la Información - SGSI.

En ese entendido, a continuación, se especifican las necesidades, expectativas y el nivel de aplicación de las partes interesadas para el ESTADO Y ALIADOS ESTRATÉGICOS:

Tabla 7.1 *Partes Interesadas.*

Parte Interesada	Necesidad	Expectativa	Aporte a SGSI	Resultados esperados	Aplica Nacional	Aplica Territorio
Min Tic	Brindar información sobre la ejecución de los planes, servicios, ejes temáticos, marco estratégico de TI y Gobierno Digital. Dar cumplimiento a los lineamientos y procedimientos en la normativa legal vigente correspondiente a seguridad y privacidad de la información. Generación de conocimiento de las nuevas amenazas emergentes en el IDARTES.	Acompañamiento en el análisis de la infraestructura con el fin de identificar vulnerabilidades en la implementación del SGSI. Fortalecer los canales de comunicación de tal forma que sea efectiva y asertiva entre los entes de control externo, con el fin de mantener informado a éstos de los distintos ataques cibernéticos, mitigando los riesgos y previniendo incidencias.	Lineamientos Normativa	Cumplimiento normativo de Gobierno Digital.	X	X
Autoridades Policiales	Generación de conocimiento de las nuevas amenazas emergentes en el IDARTES. Generar informes de los incidentes de seguridad, privacidad de la información y seguridad digital presentados en la entidad cuando se considere necesario.	Acompañamiento en el análisis de la infraestructura con el fin de identificar vulnerabilidades en la implementación del SGSI. Fortalecer los canales de comunicación de tal forma que sea efectiva y asertiva entre los entes de control externo, con el fin de mantener informado a estos de los distintos ataques cibernéticos, mitigando los riesgos y previniendo incidencias.	Políticas de Seguridad de la Información	Apoyo a Respuesta oportuna a incidentes de Seguridad de la Información que contemplan análisis forense	X	X
Equipo de Respuesta a Incidentes de	Articulación, cooperación, información y comunicación Interinstitucional.	Que el IDARTES dé cumplimiento a la normativa vigente en lo referente a seguridad de la	Políticas de seguridad de la información	Respuesta oportuna a incidentes de Seguridad de la	X	

Parte Interesada	Necesidad	Expectativa	Aporte a SGSI	Resultados esperados	Aplica Nacional	Aplica Territorio
Seguridad Informática-CSIRT	Implementar estrategias y herramientas para el intercambio de conocimiento e información. Dar a conocer los informes de alerta de ataques que se están presentando a nivel mundial y local, y que puedan afectar a alguna entidad estatal colombiana.	información, seguridad digital, privacidad y continuidad de la operación.		Información.		
Grupo de Respuesta a Emergencias Cibernéticas de Colombia-COLCERT	Articulación, cooperación, información y comunicación Interinstitucional. Implementar estrategias y herramientas para el intercambio de conocimiento e información. Brindar apoyo respecto a la Ciberseguridad de Infraestructuras Críticas del país	Que el IDARTES dé cumplimiento a la normativa vigente en lo referente a seguridad de la información, seguridad digital, privacidad y continuidad de la operación. Coordinación de emergencias ante incidentes.	Políticas de seguridad de la información	Respuesta oportuna a incidentes de Seguridad de la Información.	X	
Superintendencia de Industria y Comercio-SIC	Articulación, cooperación, información y comunicación Interinstitucional. Implementar estrategias y herramientas para el intercambio de conocimiento e información. Registro de Base de datos en el marco de la Ley 1581 de 2012.	Que el IDARTES dé cumplimiento a la normativa vigente en lo referente a seguridad de la información, seguridad digital, privacidad y continuidad de la operación.	Cumplimento de requisitos legales en materia de protección y tratamiento de datos personales.	Evitar sanciones o hallazgos por entes de control.	X	X
Ciudadanía	Protección de sus datos personales, transparencia en el uso de su información.	Que las entidades públicas garanticen la confidencialidad, integridad y disponibilidad de su información	Participación activa, reporte de incidentes, cumplimiento de trámites con datos verídicos	Confianza en la entidad, mayor transparencia, cumplimiento normativo, protección		X

Parte Interesada	Necesidad	Expectativa	Aporte a SGSI	Resultados esperados	Aplica Nacional	Aplica Territorio
				efectiva de sus datos		

Fuente: *Elaboración propia*

7.6 APLICABILIDAD

Esta política aplica a servidores públicos, contratistas y terceros del Instituto Distrital de las Artes – IDARTES, la política pretende garantizar la satisfacción de las partes interesadas priorizando la confidencialidad, integridad, disponibilidad y privacidad de la información, bajo un enfoque de mejora continua y autocontrol en los procesos y en la prestación de los servicios, con base en la sensibilización de cada uno de los servidores del Instituto Distrital de las Artes – IDARTES y el apoyo del equipo de la Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI, de manera que el acceso a la información oportuna y confiable facilite el ejercicio efectivo de los derechos constitucionales y legales, además de los controles ciudadano, político, fiscal, disciplinario y de gestión o administrativo, sin perjuicio de la reservas legales.

Esta Política se implementa a través de lo planeado y desarrollado en el Plan Estratégico de Tecnologías de la Información, Plan de Seguridad y Privacidad de la Información, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Instrumento de Medición del Modelo de Seguridad y Privacidad de la Información-MSPI y la Declaración de Aplicabilidad SoA, los cuales se revisan y actualizan de manera anual.

8. EVALUACIÓN DEL DESEMPEÑO

Conforme a la cláusula 9 de la norma ISO27001 se debe realizar el seguimiento, medición, análisis y evaluación, conforme a los controles establecidos alineados con el instrumento de *línea base de seguridad* definido por el Ministerio de las Tecnologías de la Información y las comunicaciones-MINTIC, y así, asegurar que el proceso del SGSI y los controles de seguridad de la información estén funcionando según lo previsto.

La revisión por la dirección es un elemento esencial del SGSI, será el punto formal en el que la Alta Dirección revisa la efectividad del SGSI y asegura su alineación con la dirección estratégica de la entidad, estas revisiones por la dirección deben realizarse a intervalos planificados y el programa de revisión general debe cubrir como mínimo una lista de áreas básicas especificadas en la cláusula 9.3 de la norma ISO27001.

Tabla 8.1 *Ciclo de revisión del SGSI.*

Elemento	Frecuencia	Responsable	Instrumento	Acción derivada
Revisión de políticas de seguridad	Cuando se requiera	OAPTI	Política revisada y actualizada en el sistema de calidad del IDARTES.	Ajustes a políticas, inclusión de nuevas disposiciones legales o normativas.
Evaluación de cumplimiento del MSPI	Cuatrimestral	OAPTI y CIGD	Informe de ejecución del plan de seguridad.	Implementación de acciones preventivas.

Elemento	Frecuencia	Responsable	Instrumento	Acción derivada
Auditoría interna del MSPI	Cuando se requiera	Oficina de Control Interno	Informe de auditoría interna	Mejoras al sistema, hallazgos, recomendaciones
Medición de indicadores de desempeño	De acuerdo a la programación realizada en los indicadores del MSPI	OAPTI	Tablero de indicadores del MSPI	Ajustes operacionales y de ejecución

Fuente: *Elaboración propia*

Para asegurar el cumplimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), se establecerán indicadores mínimos de evaluación que permitan medir el desempeño de los controles y procesos asociados. Estos indicadores deben incluir, entre otros:

- Número de incidentes de seguridad reportados y gestionados.
- Nivel de madurez del Modelo de Seguridad y Privacidad de la Información - MSPI.
- Nivel de sensibilización y capacitación en seguridad de la información.

Los indicadores serán evaluados con una periodicidad semestral, cuatrimestral y anual, reportados en PANDORA.

9. MEJORA

9.1 Monitoreo

La Oficina Asesora de Planeación y Tecnologías de la Información realizará el seguimiento y control a la implementación y/o mantenimiento de la Política Digital, Seguridad y Privacidad de la Información.

9.2 Mejora continua

Conforme a la cláusula 10 de la norma ISO27001:2013, la mejora se consigue aprendiendo de los incidentes de seguridad, los problemas identificados en las auditorías, los problemas de rendimiento, las quejas de las partes interesadas y las ideas generadas durante las revisiones por la dirección, y, para cada oportunidad identificada, deberá mantener registros de

- Lo que ocurrió
- Si el evento tuvo consecuencias indeseables, qué acciones se tomaron para controlarlo y mitigarlo
- La causa raíz del evento (si se determina)
- La acción tomada para eliminar la causa raíz (si es necesario)
- La evaluación de la efectividad de cualquier acción tomada.

El objetivo de la implementación del SGSI y los controles de este documento, debe ser reducir la probabilidad de que ocurran eventos de seguridad de la información, así como su impacto. Ningún SGSI es perfecto, sin embargo, dichos sistemas de gestión mejoran con el tiempo y aumentarán la resistencia frente a los ataques de seguridad de la información.

10. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Conforme a la norma ISO27001:2013 se realiza la definición de controles para fortalecer la estrategia de Seguridad Digital del IDARTES alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y el modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital. Por lo anterior se definen los dominios de la ISO 27001 y grupos de controles (administrativos y técnicos), los cuales se describen en el presente documento.

Organización de la Seguridad de la Información

10.1 Control SGSI-A.6.1 - Organización interna

Dictar lineamientos que permitan administrar la seguridad de la información dentro del IDARTES y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades y poder aplicar las medidas de seguridad adecuadas en los accesos de terceros a la información del IDARTES.

Lineamientos Generales:

- Los Roles y responsabilidades para la seguridad de la información son los dispuestos en suceso, por la cual se adopta el Modelo Integrado de Planeación y Gestión o cualquiera que la adicione, modifique o derogue.
- La información deberá estar bajo la responsabilidad del Líder de Proceso para evitar conflicto y reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de información del IDARTES.
- El Oficial de Seguridad de la Información deberá mantener contacto con las autoridades Nacionales en materia de seguridad de la información, y los boletines que estas entidades emitan deberán ser analizados y generar las acciones pertinentes conforme a la misionalidad del IDARTES.
- El Oficial de Seguridad de la Información deberá mantener los contactos apropiados con los grupos de interés especial (Policía Nacional, CSIRT, Bomberos, Defensa Civil, Grupos de atención de desastres, etc.) u otros foros de seguridad especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información, que requiera de asesoría externa.
- Todos los proyectos que se desarrollen en el marco del cumplimiento de los objetivos de los Procesos del IDARTES deberán tener un componente de seguridad de la información, el cual deberá ser acompañado y asesorado por el Oficial de Seguridad de la Información o a quien este

delegue, de acuerdo a la especificidad técnica, teniendo en cuenta las disposiciones que están estipuladas en la caracterización de la Gestión de Tecnologías de la Información.

10.2 Control SGSI-A.6.2.1 - Política para dispositivos móviles

Establecer los lineamientos para el uso, administración, consulta y operación de los servicios en los dispositivos móviles del Instituto y a su vez controlar el acceso a los mismos, en las instalaciones del IDARTES.

Lineamientos Generales:

- La OAPTI deberá establecer y divulgar los procedimientos para el uso de la información y los servicios tecnológicos del IDARTES en los dispositivos móviles tanto de propiedad del IDARTES, como aquellos suministrados por los proveedores para colaboradores en el marco de la ejecución de algún contrato o convenio, así como de propiedad de los colaboradores.
- Los dispositivos móviles que se pueden utilizar en el IDARTES son: computador portátil, celular Smartphone, Tablet. En el caso de los computadores portátiles estos deberán contar con software licenciados y antivirus actualizado, para los Smartphone y Tablet deberán utilizar la suite ofimática con las credenciales del IDARTES.
    - Los computadores portátiles de propiedad de los colaboradores no deberán estar incluidos en el dominio Idartes.gov.co, para conectarse a los servicios de la red de datos del IDARTES deberán realizar solicitud a la mesa de servicio y automáticamente se comprometen a cumplir con los lineamientos referentes a seguridad de la información.
    - En caso de que el colaborador deba hacer uso de equipos ajenos al IDARTES, estos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red del IDARTES una vez esté avalado por el grupo de Tecnología de la OAPTI, y será el grupo de TI quien deberá realizar la revisión de los requisitos antes mencionados de manera periódica en los equipos autorizados para conectarse a las redes de conectividad y datos del IDARTES.
- Los dispositivos móviles propiedad del IDARTES deberán cumplir con la política de control de acceso, y los colaboradores que deseen configurar sus dispositivos personales deberán acogerse a las políticas de monitoreo del dispositivo móvil, sin que esto incurra en una violación a la privacidad del colaborador.
- Las redes inalámbricas de funcionarios deben ser unificadas en su SSID y contraseña, permitiendo que únicamente se conecten los dispositivos móviles propiedad del IDARTES independientemente de donde sea el colaborador.
- Aquellos dispositivos móviles que son propiedad de los colaboradores o visitantes deberán conectarse a la red de Visitantes, cumpliendo con los lineamientos de la política digital, seguridad y privacidad de la información.
- La OAPTI en sus documentos de gestión del proceso dará los lineamientos de uso de la infraestructura y acceso a redes para gestionar los riesgos que conlleva el uso de dispositivos móviles.
- La OAPTI a través del Oficial de Seguridad de la Información y el servicio de seguridad informática establecerá los lineamientos para la gestión de ciberseguridad en el marco del Sistema de Gestión de Seguridad de la Información y continuidad de la operación tecnológica del IDARTES.

- Los colaboradores de terceras partes solo podrán utilizar los dispositivos asignados por el operador/contratista, para el ejercicio de las obligaciones propias del contrato suscrito con el IDARTES, cumpliendo con las directrices referentes a seguridad de la información.
- Los colaboradores en modo o conectados vía VPN se les deberán aplicar los permisos de navegación y control de acceso limitado a su perfil o privilegios, y se llevará registro de su conexión.
- Todo dispositivo móvil institucional, que transmita y/o almacene información clasificada y/o reservada de la Entidad, podrá ser monitoreado a través de la herramienta de gestión tecnológica definida por la OAPTI.
- Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la Entidad, y que transmita y/o almacene información clasificada y/o reservada, podrá ser monitoreado a través de la herramienta tecnológica definida por la OAPTI.

10.3 Control SGSI-A.6.2.2 Política para teletrabajo

Establecer los lineamientos en materia del Sistema de Gestión de Seguridad de la Información que tiene los colaboradores del IDARTES que se acogen a la modalidad de Teletrabajo para el uso, administración, consulta y operación de los servicios en las áreas de Teletrabajo.

Lineamientos Generales:

- La OAPTI deberá establecer y divulgar el uso de la información y los servicios tecnológicos necesarios para garantizar el adecuado funcionamiento de la modalidad de Teletrabajo.
- Los computadores de propiedad de los colaboradores, se les debe realizar la verificación de los requerimientos tecnológicos del equipo mediante el formato establecido por la OAPTI previa gestión de Talento Humano y la Mesa de servicio.
- Los computadores portátiles propiedad de los colaboradores deberán cumplir con la política de control de acceso a redes.
- La OAPTI será la responsable de gestionar los riesgos de seguridad de la información que se identifiquen en la modalidad de Teletrabajo y así mismo proporcionar los controles que sirvan para mitigarlos.
- La OAPTI apoyara a la Oficina de Talento Humano para verificar que los equipos personales de los colaboradores que realizan actividades de Teletrabajo cumplan con los lineamientos referentes a seguridad de la información, teniendo en cuenta lo enmarcado en la normativa y los procedimientos de Teletrabajo definidos por la Entidad.
- La OAPTI deberá implementar los controles necesarios que permitan el acceso remoto a las aplicaciones o servicios tecnológicos del IDARTES a los colaboradores que realicen actividades en Teletrabajo, así mismo se deben tener en cuenta la revocación de servicios cuando el colaborador no continué realizando actividades de Teletrabajo.
- Los colaboradores en modo Teletrabajo o conectados vía VPN se les deberán aplicar los permisos de navegación y control de acceso limitado a su perfil o privilegios y se llevará registro y seguimiento de su conexión.

Seguridad del Recurso Humano

10.4 Control SGSI-A.7.1.1 - Selección

Dictar lineamientos para que el personal que se contrata cumpla con las políticas del IDARTES en materia de seguridad de la información.

Lineamientos Generales:

- El Grupo de Talento Humano deberá definir formalmente un mecanismo de verificación del personal en el momento en que se postula al cargo. Dicho mecanismo deberá incluir los aspectos legales y procedimentales de vinculación del IDARTES y los que dicte la Función Pública.
- La Oficina Jurídica deberá definir una lista de verificación que contenga los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con lo que dicta la ley y la reglamentación vigente.
- Los procesos de selección de personal de planta y procesos contractuales deberán contener la autorización para el tratamiento de los datos personales de acuerdo con la política de tratamiento de datos personales del IDARTES y de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
- Los documentos de verificación deberán reposar en la historia laboral o carpeta contractual del colaborador.
- La Oficina de Talento Humano y la Oficina Jurídica deberán establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.

10.5 Control SGSI-A.7.1.2 - Términos y condiciones del empleo

Dictar lineamientos para que el personal que se vincula o se contrata cumpla con las políticas del IDARTES en materia de seguridad de la información.

Lineamientos Generales:

- La Oficina Jurídica deberá definir los términos y condiciones del contrato, en los cuales se establecerán las obligaciones del contratista en materia de seguridad de la información, las leyes de propiedad intelectual, de protección de datos personales, de transparencia y acceso a la información pública.
- El Grupo de Talento Humano y la Oficina Jurídica deberán dar a conocer a los colaboradores los términos y condiciones de empleo o contrato y especificar las responsabilidades u obligaciones en materia de la seguridad de la información y aclarar que estas se extienden más allá de los límites del IDARTES y del horario normal de trabajo o de ejecución del objeto contractual.

- La Oficina Jurídica deberá incluir en el pliego de condiciones o estudios previos para la contratación de terceras partes, las obligaciones referentes a las políticas, lineamientos y directrices en materia de seguridad de la información que dicte el IDARTES y aquellas contenidas en las guías para la adquisición de bienes y servicios de calidad.
- El Grupo de Talento Humano y la Oficina Jurídica deberán hacer firmar un documento de compromiso de confidencialidad de la información a los colaboradores, dicho documento debe reposar en la historia laboral o expediente contractual según sea el caso.

10.6 Control SGSI-A.7.2.1 - Responsabilidades de la Dirección

Dictar lineamientos a todos los colaboradores del IDARTES en la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.

Lineamientos Generales:

- El supervisor del contrato deberá hacer seguimiento al cumplimiento de las obligaciones generales de todos los contratos en materia de seguridad de la información, sin importar su naturaleza.
- La OAPTI dará a conocer la Política Digital, Seguridad de la Información a los colaboradores del IDARTES.
- Una vez formalizado el proceso de vinculación, el supervisor de contrato o jefe inmediato solicitará la creación de la cuenta de usuario y apertura del inventario de vinculación del personal a través del colaborador conforme al procedimiento de Gestión de Usuarios aprobado y publicado.
- La Oficina Jurídica, Talento Humano, el supervisor del contrato o el jefe inmediato deberá informar a la Mesa de servicio sobre las novedades del colaborador para tomar las acciones pertinentes.

10.7 Control SGSI-A.7.2.2 - Toma de conciencia y formación en la seguridad de la información

Dictar lineamientos para que los colaboradores del IDARTES sean sensibilizados en temas del Modelo de seguridad y Privacidad de la Información - MSPI, buenas prácticas y toma de conciencia.

Lineamientos Generales:

- El Grupo de Talento Humano, deberá propender que los colaboradores del IDARTES y usuarios de terceras partes que desempeñen funciones en el mismo reciban entrenamiento y actualización periódica en materia de Seguridad de la Información.
- La OAPTI a través del Oficial de Seguridad de la Información, diseñará e implementará un plan con estrategias de cultura, cambio y apropiación referentes al Modelo de seguridad y privacidad de la información.
- El Grupo de Talento Humano, realizará las acciones para realizar cursos del Sistema Integrado de Gestión – SIG contenido en la escuela virtual del IDARTES referentes al tema MSPI.

10.8 Control SGSI-A.7.2.3 - Proceso disciplinario

Dictar lineamientos para generar acciones a los colaboradores que hayan cometido un desacato a la seguridad de la información.

Lineamiento General:

En lo pertinente al incumplimiento y desacato de las políticas de la seguridad y privacidad de la información, se aplicará lo establecido en los procedimientos destinados para tal fin, por los entes de control interno del IDARTES.

10.9 Control SGSI-A.7.3.1 - Terminación o cambio de responsabilidades de empleo

Dictar lineamientos para las responsabilidades y deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo.

Lineamientos Generales:

- El supervisor del contrato o a quien delegue deberá recoger y custodiar activos e información del IDARTES, bajo la responsabilidad de los contratistas, en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
- El jefe inmediato o a quien delegue deberá recoger y custodiar la información del IDARTES en el caso de retiro, investigación, inhabilidades, o cambio de funciones.
- El jefe inmediato o el supervisor del contrato a través de canales oficiales deberán informar a la OAPTI a través de la Mesa de servicio, cualquier novedad de desvinculación administrativa, laboral o contractual del colaborador; una vez notificada la novedad la OAPTI deberá proceder a la inactivación de los accesos del colaborador, teniendo en cuenta los parámetros y directrices definidos en el procedimiento de Gestión de Usuarios.

10.10 Control SGSI-A.8.1.1 – A.8.1.2 - Inventario y propiedad de los activos

Identificar los activos de información del IDARTES, manteniendo un inventario de estos.

Lineamientos Generales:

- En el marco del proyecto PETI referente al MSPI deberá aplicar y mantener actualizada la documentación para el levantamiento y actualización de los activos de Información del IDARTES.
- Los líderes de los procesos deberán mantener un inventario de sus activos de información de forma anual y serán actualizados según el evento en que se requiera.
- El IDARTES deberá designar responsabilidades a los líderes de los procesos sobre sus activos de información.
- El Líder de Seguridad de la Información, deberá remitir el consolidado del levantamiento de activos de información, a la Dependencia designada por la Dirección General que lidera la estrategia de la Ley de transparencia y acceso a la información pública y la estrategia de

Gobierno Digital o a quien haga sus veces, con el objetivo de ser analizada, realimentada, actualizada y publicada de acuerdo a la normativa vigente colombiana teniendo en cuenta los lineamientos de legalidad emitidos por la Oficia Jurídica.

10.11 Control SGSI-A.8.1.3 - Uso aceptable de los activos

Dictar lineamientos para identificar, documentar e implementar las reglas para el uso aceptable de información.

Lineamientos Generales:

- Los colaboradores y usuarios de partes externas deberán utilizar únicamente los aplicativos y equipos de cómputo autorizados por la OAPTI.
- En caso de que el colaborador deba hacer uso de equipos ajenos al IDARTES, estos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red del IDARTES una vez esté avalado por la OAPTI.

- El único servicio de correo electrónico autorizado para la gestión de información institucional en el Instituto Distrital de las Artes – IDARTES es aquel que utiliza el dominio @idartes.gov.co. No obstante, debido a consideraciones presupuestales y en el marco de las políticas de austeridad, se podrán asignar cuentas de correo personal exclusivamente a contratistas que no manejen información sensible, confidencial o sujeta a reserva.

  El uso de cuentas de correo electrónico personales solo se permitirá en casos excepcionales, debidamente justificados y documentados, y bajo el principio de no tratamiento de información crítica. Esta medida busca minimizar los riesgos asociados a filtraciones de datos, garantizando un entorno seguro para el intercambio de información institucional.

- El IDARTES podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado en caso de posible desacato a las leyes, decretos o reglamentación interna del IDARTES.
- Las firmas de documentos oficiales que se constituyan como activos de información de acuerdo a la tabla de retención documental o acto administrativo deben reposar en original o con firma digital, en ningún caso se debe utilizar firmas digitalizadas o escaneadas, salvo en aquellos que se autorice por acto administrativo de la Dirección General, indicando para qué fin y porqué medios (comunicados masivos individuales a los aportantes, comunicaciones masivas individuales a colaboradores u operadores, entre otros).
- El IDARTES se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucionales, de todos sus funcionarios o contratistas, además podrá realizar copias de seguridad en cualquier momento, así como limitar el acceso temporal o definitivo, por solicitud expresa del coordinador, ordenador(a) del gasto, supervisor del contrato, jefe inmediato, Director(a) General, Jefe de Oficina de Control Interno Disciplinario o Director(a) de Talento Humano a la OAPTI, así como a todos los servicios y accesos a sistemas de información de la Entidad o de terceros operados en la Entidad.
- Con el fin de mitigar la suplantación de correos electrónicos, se prohíbe suministrar acceso directo a los buzones de correo asignado a cada colaborador. En caso de ser necesario realizar la gestión del correo institucional, se debe solicitar a la mesa de servicio listando los colaboradores que tendrán los permisos para escribir correos en nombre del colaborador solicitante.

- Se recomienda y prioriza el uso de firma digital o firma electrónica con autenticación de terceros confiables (prestadores de servicios de certificación digital acreditados) para garantizar la validez jurídica, seguridad y trazabilidad de los documentos institucionales.

10.12 Control SGSI-A.8.1.4 - Devolución de activos

Todos los colaboradores y terceras partes deberán devolver todos los activos de información del IDARTES que se encuentren a su cargo al terminar su empleo, contrato o vínculo laboral.

Lineamientos Generales:

- Los colaboradores y terceras partes deberán devolver todos los activos de información del IDARTES que se encuentran en su poder a la terminación de su empleo, contrato, convenio o vínculo laboral.
- Para el traslado de equipos de cómputo al almacén o a otros colaboradores, o baja de los inventarios por cualquier motivo, se deberá realizar un respaldo de la información que en él se encuentre, a través de la mesa de servicio. Posteriormente se debe seguir el Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo, en los equipos que contengan medios de almacenamiento con el fin de propender que la información del IDARTES contenida en estos medios no se pueda recuperar.
- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro será la OAPTI, sin embargo, cuando deba realizarse desde y hacia el almacén será la Dirección Administrativa, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la Entidad.

10.13 Control SGSI-A.8.2.1 - Clasificación de la información

Clasificar la información de acuerdo con los requisitos legales, valor y criticidad de la información.

Lineamientos Generales:

- Los propietarios de la información son los encargados de realizar la clasificación de la información.
- El IDARTES definirá los niveles adecuados para clasificar su información de acuerdo con su sensibilidad donde se valorarán por confidencialidad o integridad o disponibilidad de la información, a través de la guía de gestión y clasificación de activos de información. Estos niveles deberán ser oficializados y divulgados a los colaboradores.
- Los custodios son responsables de aplicar los controles para la protección de la información según su nivel de clasificación.
- Si la información es de carácter clasificada o reservada y es requerida por algún ente externo o ciudadano en donde opere el IDARTES, su entrega está supeditada a la aprobación previa de su propietario y de las instancias jurídicas o administrativas establecidas.

- Los propietarios y custodios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su reclasificación.
- Los colaboradores y terceras partes deberán acatar los lineamientos definidos para la rotulación de la información, para divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física del IDARTES.
- La información física y digital del IDARTES deberán tener un periodo de almacenamiento que puede ser dado por requerimientos legales o misionales; este periodo deberá ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información deberá ser eliminada adecuadamente.

10.14 Control SGSI-A.8.2.2 - A.8.2.3 - Etiquetado de la información manejo de activos

La OAPTI a través de la estrategia de Seguridad de la Información, la Subdirección Administrativa y Financiera y Financiera a través de la oficina de Gestión Documental y con el apoyo de la Oficina Jurídica, dictarán los lineamientos para desarrollar e implementar los procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por IDARTES.

Lineamientos Generales:

- Los colaboradores deberán aplicar lineamientos para la rotulación de la Información.
- Las series y subseries de las Tablas de Retención Documental (TRD) deberán contener en su estructura el tipo de clasificación.
- Cada Propietario de la Información velará por el cumplimiento establecido en los lineamientos para la rotulación de la información.
- La Subdirección Administrativa y Financiera y Financiera a través de la oficina de Gestión Documental, y la OAPTI deberán establecer controles para mantener protegida la información física y electrónica durante su ciclo de vida.

10.15 Control SGSI-A.8.3.1 - Gestión de medios removibles

Dictar lineamientos para implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por el IDARTES.

Lineamientos Generales:

La OAPTI a través de la Oficina de Recursos Tecnológicos, establecerá los siguientes lineamientos:

- Un instructivo para el uso de medios removibles.
- En ninguna circunstancia se dejará desatendido los medios de almacenamiento copias de seguridad de los sistemas de información.

- Los colaboradores que hagan uso de token para el desempeño de sus funciones u obligaciones deberán velar por la custodia y buen manejo de estos.
- Deberá proveer los métodos de cifrado de la información además de suministrar el software o herramienta utilizado para tal fin.
- Todo medio removible deberá ser escaneado mediante antivirus cada vez que se conecte a un equipo de la red del IDARTES.
- Es responsabilidad de cada colaborador tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío de este.
- Se prohíbe el uso de medios removibles en lugares de acceso al público que contengan información reservada o clasificada del IDARTES.
- Para la disposición final de residuos de aparatos electrónicos, se debe dar cumplimiento a lo establecido en el lineamiento para manejo de Residuos Especiales.
- En caso de residuos de aparatos eléctricos y electrónicos como discos duros, se debe realizar la eliminación de la información a través de borrado seguro, antes de aplicar el Procedimiento o formato de manejo de residuos especiales. Cuando un Disco Duro por su obsolescencia o daños irreparables se dañe y sea imposible realizar el borrado seguro se debe garantizar que la información no sea recuperable.

10.16 Control SGSI-A.8.3.2 - Disposición de los medios

Disponer de forma segura de los medios cuando estos no se requieran, aplicando buenas prácticas ambientales y de seguridad de la información.

Lineamientos Generales:

La OAPTI desarrollará lineamientos para la disposición de medios teniendo en cuenta lo siguiente:

- Los equipos que se regresen al almacén para asignarse a otro colaborador o para dar de baja, se les deberá seguir el Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo, en caso de no poder realizar el borrado de información validar el lineamiento de manejo de residuos especiales.
- Se deberán emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los equipos que contengan medios de almacenamiento y que serán reutilizados o eliminados, con el fin de controlar que la información del IDARTES contenida en estos medios no se pueda recuperar, esta solicitud deberá ser mediante solicitud a la mesa de servicio, con aprobación del jefe inmediato o supervisor de contrato.
- Es requisito realizar el respaldo o copia de la información contenida en el equipo, previa ejecución del borrado de información.

10.17 Control SGSI-A.8.3.3 - Transferencia de medios físicos

Dictar lineamientos para proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte de los medios que contienen información.

Lineamientos Generales:

La OAPTI establecerá los lineamientos para mantener la seguridad de la información que se transfiere dentro del IDARTES y con cualquier entidad externa teniendo en cuenta lo siguiente:

- Cuando se requiera transferir un medio de almacenamiento de información del IDARTES a otras entidades se deberá establecer un acuerdo entre las partes.
- Dichos acuerdos deberán dirigirse a la transferencia segura de información de interés entre el IDARTES y las partes.
- Cuando se requiera transferir un medio de almacenamiento se deberá tener en cuenta el registro de contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte y la entrega.
- Los colaboradores y terceras partes que interactúan en procesos de intercambio de información al exterior del IDARTES deberán cumplir los lineamientos, recomendaciones o estrategias establecidas para este propósito.
- El transporte para los medios de almacenamiento deberá contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información

Control de Acceso

10.18 Control SGSI-A.9.1.1 – A.9.1.2 - Política de control de acceso - Acceso a redes y a servicios de red

Definir parámetros para establecer, documentar controles de acceso con base en los requisitos del IDARTES, así mismo establecer permisos de acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados.

Lineamientos Generales:

La OAPTI define los lineamientos para la política de control de acceso, el acceso a redes y servicios en red teniendo en cuenta lo siguiente:

- La OAPTI suministrará a los usuarios las credenciales respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, de esta forma las credenciales de acceso son de uso personal e intransferible.
- Es responsabilidad de los colaboradores o terceras partes del IDARTES el manejo que se les dé a las credenciales de acceso asignadas.

- Los colaboradores o terceras partes que realicen actividades administrativas sobre la plataforma tecnológica del IDARTES, las deberán realizar en las instalaciones del Instituto y no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del supervisor del contrato.
- La conexión remota a la red de área local del IDARTES deberá establecerse a través de una conexión VPN suministrada por el IDARTES, la cual deberá ser aprobada, registrada y auditada por la OAPTI.
- La OAPTI deberá realizar revisiones e inactivaciones de las conexiones VPN cada treinta (30) días o de acuerdo con las solicitudes de desactivación generadas en la mesa de servicio.
- Las conexiones remotas deberán utilizar los métodos establecidos de autenticación para el control de acceso de los usuarios.
- Deberá establecer una adecuada segregación de redes, separando los entornos de red de usuarios de los entornos de red de servicios.
- Deberá establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos, los recursos y servicios del IDARTES.
- El control de acceso a los datos, información y servicios se deberá basar en el principio del menor privilegio, lo que implica que no se otorgará acceso a menos que sea explícitamente permitido.
- Deberá crear, modificar y deshabilitar las cuentas de acceso o recursos del IDARTES de acuerdo con el procedimiento establecido.
- Deberá verificar periódicamente los controles de acceso para los usuarios del IDARTES y los provistos a terceras partes, con el fin de revisar que dichos usuarios tengan los permisos únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.
- Los equipos personales de los colaboradores que se conecten a las redes de datos del IDARTES deberán cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.
- No se podrá utilizar ningún tipo de utilitario para conexión remota a la red interna del IDARTES, únicamente se deberá utilizar el designado por la OAPTI del IDARTES.

Usuario local equipos portátiles

- Los usuarios locales serán configurados en los equipos portátiles, considerando que estos dispositivos están diseñados para facilitar la movilidad y uso fuera de las instalaciones, lo que requiere configuraciones adaptadas para su operación en diferentes ubicaciones.
- La sesión local de los equipos portátiles tendrá una contraseña asignada por la OAPTI, razón por la cual los usuarios no tienen autorización de modificar la contraseña.
- La creación de los usuarios locales debe cumplir con las políticas de Seguridad de la Información del IDARTES y sólo se autorizará cuando sea estrictamente necesario para el funcionamiento de actividades específicas, su uso debe ser cuidadosamente controlado y gestionado para minimizar los riesgos asociados.
- Las cuentas de usuarios locales deberán tener restricción de privilegios según el principio de "mínimos privilegios".

Responsabilidad del usuario de la cuenta local

El usuario que haga uso de una cuenta local en los portátiles será el responsable de la protección de la Confidencialidad, Integridad y Disponibilidad de la información a la que tenga acceso mediante dicha cuenta. Esto implica que el usuario debe:

- **Confidencialidad:** Proteger la información a la que acceda y no compartir sus credenciales de acceso con terceros.
- **Integridad:** Asegurar que no se realicen alteraciones no autorizadas en la información.
- **Disponibilidad:** Garantizar el acceso adecuado a la información en función de las necesidades de su actividad laboral, evitando la obstrucción, modificación, robo o pérdida de acceso a la misma.

Riesgos asociados al uso incorrecto del usuario de la cuenta local

El usuario es consciente y acepta los riesgos de Seguridad de la Información que pueden materializarse por uso incorrecto de la cuenta local, los cuales incluyen, pero no se limitan a:

- Exposición no autorizada de datos sensibles.
- Modificación o eliminación de información crítica.
- Interrupción en la disponibilidad de los sistemas y servicios.
- Explotación de vulnerabilidades por no adherirse a los protocolos de seguridad establecidos.
- Accesos a recursos no autorizados.
- Ataques internos.
- En caso que se detecte que un funcionario y/o contratista o colaborador haya incurrido en el uso incorrecto de una cuenta local, el cual genere un incidente de Seguridad de la Información, el IDARTES podrá iniciar un proceso disciplinario para asegurar que se tomen las medidas adecuadas y que se mantenga la integridad y seguridad de la información de la entidad.

Medidas preventivas y correctivas

El usuario de la cuenta local deberá seguir las prácticas y lineamientos recomendados de seguridad de la Información establecidas en el IDARTES, como el uso de contraseñas robustas, la actualización periódica de las mismas y el bloqueo de sesiones inactivas.

- Cualquier incidente de seguridad relacionado con el uso indebido o incorrecto de la cuenta local deberá ser reportado inmediatamente a la mesa de servicios del IDARTES.
- En caso de que se identifique un incidente relacionado con el uso incorrecto de la cuenta local que comprometa la seguridad de la información, el usuario será considerado responsable y deberá colaborar en la investigación y mitigación de los daños.

10.19 Control SGSI-A.9.2.1 Registro y cancelación del registro de usuarios

Dictar lineamientos para el registro y cancelación de usuarios del IDARTES.

Lineamientos Generales:

La OAPTI establece los lineamientos para el registro y cancelación de usuarios teniendo en cuenta lo siguiente:

- Deberá definir un procedimiento para el registro y la cancelación de usuarios en el IDARTES, teniendo en cuenta que las identificaciones de los usuarios deberán ser únicas.

- Deberá definir un estándar para la creación de las cuentas de usuario institucionales.
- Deberá deshabilitar las credenciales de acceso a los colaboradores que no tengan ningún vínculo laboral o contractual con el IDARTES.

10.20 Control SGSI-A.9.2.2 Suministro de acceso de usuarios

Definir los lineamientos para el proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para los sistemas y servicios del IDARTES.

Lineamientos Generales:

La OAPTI establecerá los lineamientos para el proceso de suministro de acceso formal o revocar los derechos de acceso de usuarios teniendo en cuenta lo siguiente:

- El acceso a la información del IDARTES es otorgado sólo a usuarios autorizados, teniendo en cuenta lo requerido para la realización de sus labores relacionadas con su responsabilidad o tipo de servicio con los privilegios asignados.

Definir los controles de seguridad a los tipos de usuarios dependiendo el acceso a la información que este requiera:

- Usuario Proveedor o Tercero: son aquellos usuarios externos al IDARTES que prestan un servicio bajo un contrato y requieren acceso a la plataforma tecnológica de la entidad.
- Usuario Especial: son usuarios externos que requieren acceso a la plataforma de la entidad para una actividad específica, como los entes de control, estos usuarios deberán ser solicitados por la Oficina de Control Interno del IDARTES con los respectivos permisos siguiendo el procedimiento estipulado.
- Usuario Administrador: son los usuarios funcionarios, contratistas o terceros que por sus funciones u obligaciones requieren permisos de administración para el desarrollo de sus actividades en la plataforma de la entidad.
- Usuario Institucional: son los usuarios estándar como contratistas, pasantes y funcionarios de planta entre otros.
- No se deberá configurar el acceso a los recursos tecnológicos a usuarios que no hayan formalizado el proceso de ingreso al IDARTES.
- Todo usuario que quiera acceder a servicios o información de la plataforma tecnológica del IDARTES deberá autenticarse.
- Los usuarios deberán cumplir con los lineamientos para la creación y uso de contraseñas.
- El uso de credenciales de usuarios administradores de sistemas operativos, consolas de administración y bases de datos tales como: “root”, “adm”, “admin”, “administrador”, “SQLAdmin”, “administrator” y “system”, entre otros, deberán ser controladas, monitoreadas, vigiladas y custodiadas por los administradores asignados de los sistemas y servicios tecnológicos de la OAPTI.

- Todos los colaboradores y terceras partes deberán cumplir las condiciones de acceso y mantener de forma confidencial las contraseñas con la finalidad de preservar el no repudio.

10.21 Control SGSI-A.9.2.3 Gestión de derechos de acceso privilegiado

Dictar lineamientos para restringir y controlar la asignación y uso de derechos de acceso privilegiado.

Lineamientos Generales:

La OAPTI desarrollará los lineamientos para restringir y controlar la asignación y uso de derechos de acceso
privilegiado teniendo en cuenta lo siguiente:

- Deberá otorgar los privilegios para la administración de recursos tecnológicos, servicios de red y sistemas de información, únicamente a aquellos colaboradores que cumplan dichas funciones.
- Deberá otorgar cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información, diferentes a los nativos y deberán ser cuentas únicas asociadas al usuario de dominio del administrador.
- Deberá restringir las conexiones remotas a los recursos de la plataforma tecnológica y se deberá permitir únicamente el acceso a los colaboradores autorizados.
- Deberán deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, el firmware y las bases de datos.
- Deberá mantener un listado actualizado con las cuentas que administren todos los recursos tecnológicos del IDARTES.
- Cada unidad de gestión dentro del IDARTES deberá asignar un responsable para administrar los privilegios en las carpetas asignadas en el servicio de almacenamiento con el que dispone el IDARTES, este deberá ser reportado a la OAPTI como administrador del espacio de almacenamiento.
- No se permite que los usuarios tengan carpetas compartidas en sus equipos, para ello debe hacer uso de los recursos que tiene el IDARTES.
- Los administradores de carpeta serán los responsables de los accesos y asignación de permisos (lectura, escritura, modificación y eliminación) de las carpetas y subcarpetas asignadas, los cuales deberán tener sus respectivos soportes.

La OAPTI deberá:

- Generar registros de auditoría que contengan eventos relacionados de seguridad, teniendo en cuenta criterios tales como nombre de usuario, fechas y hora de evento, tipo de modificación sobre el objeto. Se deberá realizar un respaldo de esta información facilitando la revisión y el análisis de estos.

- Establecer controles que permitan validar que solo cuenten con los permisos de acceso los usuarios autorizados.
- Realizar respaldo a toda la información alojada dentro de las carpetas y subcarpetas de acuerdo con la ley 594 de 2000 Ley General de Archivo y/o cualquiera que la derogue o modifique, adicionalmente se tendrá en cuenta el sistema de gestión documental del IDARTES.
- Realizar monitoreo permanente al servicio de almacenamiento esto con el fin de evitar fallas y en caso de existir reportarlas de manera oportuna.
- Contar con herramientas que le permitan detectar fallas en la solución de almacenamiento y tomar las medidas correctivas necesarias.
- Establecer cuotas de almacenamiento para cada recurso compartido, adicional a esto se deberá definir umbrales que permitan notificar al administrador del servicio de almacenamiento y al administrador de carpeta que el espacio asignado ya está llegando a su límite. Cada cuota está sujeta a las necesidades de cada área y a la proyección de crecimiento de cada una de ellas.

10.22 Control SGSI-A.9.2.5 Revisión de los derechos de acceso de usuarios

Dictar lineamientos para que se realice la revisión de los derechos de acceso de los usuarios a intervalos regulares.

Lineamientos Generales:

- La OAPTI deberá generar reportes de uso de cada uno de los sistemas de información con el fin de identificar la periodicidad de uso de cada uno de los usuarios.
- La OAPTI deberá revisar los derechos de acceso de los usuarios administradores por lo menos dos veces al año.

10.23 Control SGSI-A.9.2.6 Retiro o ajuste de los derechos de acceso

Dictar lineamientos para el retiro o cambios de los derechos de acceso de todos los colaboradores y terceras partes a la información y a las instalaciones de procesamiento de información.

Lineamientos Generales:

La OAPTI establecerá los lineamientos para que se realice el retiro y cambios de los derechos de acceso a todos los colaboradores y terceras partes a la información y a las instalaciones de procesamiento de información teniendo en cuenta lo siguiente:

- El retiro de los privilegios se deberá hacer inmediatamente se realice la solicitud de desactivación.
- Es responsabilidad de la oficina de Talento Humana o a quien esta delegue, de los supervisores de los contratos dar a conocer a la OAPTI el retiro, suspensión o cualquier novedad administrativa que se presente con los usuarios del IDARTES, esta novedad se deberá reportar a través de los canales establecidos de la mesa de servicio.

10.24 Control SGSI A.9.3.1 – A.9.4.3 - Uso de información secreta para la autenticación y gestión de contraseñas

Dictar lineamientos para la asignación de información de autenticación secreta, concienciando y controlando que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de contraseñas.

Lineamientos Generales:

La OAPTI establece los lineamientos para la asignación de información de autenticación secreta teniendo en cuenta lo siguiente:

- Los usuarios son responsables del uso de las contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos del IDARTES.
- El cambio de contraseña solo podrá ser solicitada por el titular de la cuenta o jefe/supervisor inmediato.

  Las contraseñas:
  - Deberán poseer un grado de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, entre otros.

Deberá cumplir con las siguientes recomendaciones como mínimo:

- Tener como mínimo diez (10) caracteres alfanuméricos sin repetición.
- No deberá contener el nombre de usuario, el nombre real o la sigla IDARTES.
- Los números que contengan no deberán ser consecutivos No se deberán usar contraseñas con los nombres de los hijos, esposo, mascotas, fechas de aniversarios, cumpleaños, etc.
- Deberán ser diferentes de otras contraseñas anteriores proporcionadas, es decir las ultimas diez (10) suministradas al dominio no se deberán repetir.
- No se deberán usar las mismas contraseñas de la autenticación para uso personal.
- Deberán estar compuestas por: letras en mayúsculas “A, B, C…”, letras en minúsculas “a, b, c…”, números “0, 1, 2, 3…”, símbolos especiales “@, #, $, %, &, (), ¡, !, ¿, ?, <>…” y espacios en cualquier orden.
- Deberán cambiarse obligatoriamente cada 60 días o cuando lo establezca los lineamientos de la OAPTI.
- Después de 3 (tres) intentos no exitosos de ingreso de la contraseña el usuario deberá ser bloqueado de manera inmediata y deberá esperar un tiempo determinado para volver a intentar, o solicitar el desbloqueo a través de la mesa de servicio.
- Deberá cambiarse si se ha detectado anomalía o incidencia en la cuenta del usuario.
- Deberá no ser visible en la pantalla, al momento de ser ingresada.
- No deberán ser reveladas a ninguna persona.
- No se deberá registrar en papel, correo electrónico, archivos digitales a menos que se puedan almacenar de forma segura y el método de almacenamiento esté aprobado por la OAPTI.

10.25 Control SGSI-A.9.4.1 Restricción de acceso a la información

Dictar lineamientos para el acceso a la información y a la funcionalidad de las aplicaciones.

Lineamientos Generales:

La OAPTI deberá definir los lineamientos para la restricción de acceso a la información teniendo en cuenta lo siguiente:

- Deberá implementar controles para que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
- Deberá establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, deberá implementar para los desarrolladores internos o externos acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- Deberá proporcionar repositorios de archivos fuente de los sistemas de información; estos deberán contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
- Los desarrolladores deberán asegurar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- Los desarrolladores deberán establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cuál fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
- Los desarrolladores deberán asegurar que no se despliegan en la pantalla las contraseñas ingresadas.
- Los desarrolladores deberán asegurar que se inhabiliten las cuentas de acuerdo con lo que establece el control SGSI A.9.3.1 – A.9.4.3, estipulado en esta política.
- Los desarrolladores deberán asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deberán tener un periodo de validez establecido; se deberán forzar el cambio de las contraseñas temporales después de su utilización inicial.
- Los desarrolladores deberán establecer que periódicamente se revalide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados sin autorización.
- El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deberán estar restringidos y estrictamente controlados.
- Las sesiones inactivas deberán cerrarse después de un período de inactividad definido y se deberán usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones misionales de alto riesgo.
- Deberá integrar las aplicaciones con el Directorio Activo, en el caso de usuarios externos estos deberán autenticarse mediante mecanismos de identificación única y en los procesos de criticidad de información se establecerá con el área funcional u operativa un mecanismo de autenticación.

10.26 Control SGSI-A.9.4.2 Procedimiento de ingreso seguro

Definir lineamientos para un proceso de ingreso seguro a los sistemas y las aplicaciones del IDARTES.

Lineamientos Generales:

- Después de tres (3) minutos de inactividad del sistema, se considerará tiempo muerto y se deberá bloquear la sesión sin cerrar las sesiones de aplicación o de red.
- Para el caso de aplicaciones o sistemas de información específicos el sistema se bloquea después de veinte (20) minutos de inactividad.

El acceso a los sistemas o aplicaciones deberá estar protegido, mediante un inicio seguro de sesión, que contempla las siguientes condiciones:

  - No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
  - No suministrar mensajes de ayuda, durante el proceso de autenticación.
  - Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.

- Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos hasta un máximo de tres (3) intentos.
- No mostrar las contraseñas digitadas con anterioridad.
- No transmitir la contraseña en texto claro.
- Todo acceso a un sistema de información o a un recurso informático deberá registrarse y mantenerse respaldado.

10.27 Control SGSI-A.9.4.4 Uso de programas utilitarios especiales

Definir lineamientos para restringir y controlar el uso de programas utilitarios privilegiados que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

Lineamientos Generales:

La OAPTI establece los lineamientos para el uso de programas utilitarios privilegiados teniendo en cuenta lo siguiente:

- Deberá establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información, no tengan instalados en sus equipos de cómputo utilitarios que permitan escalar privilegios o evadir controles de seguridad informáticos.
- Deberá monitorear a los administradores de los recursos tecnológicos y servicios de red, para que no hagan uso de utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para anular la seguridad de los sistemas de información alojados sobre la plataforma tecnológica.
- Deberá generar y mantener actualizado un listado de programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información.
- Deberá retirar o deshabilitar los programas utilitarios privilegiados no autorizados de la plataforma tecnológica, los servicios de red y sistemas de información.

10.28 Control SGSI-A.9.4.5 Control de acceso a códigos fuente de programas

Definir lineamientos con respecto al acceso a los códigos fuentes de los sistemas de información del IDARTES.

Lineamientos Generales:

La OAPTI desarrollarán los lineamientos para el control de acceso a códigos fuente teniendo en cuenta lo siguiente:

- El acceso al código fuente del programa es limitado, solamente el arquitecto de software y los ingenieros desarrolladores y de soporte serán autorizados por la OAPTI.

  - Acceso Restringido: Sólo un grupo selecto de desarrolladores autorizados debe tener permiso para acceder al código fuente. Esto implica que las entidades deben implementar controles rigurosos para asegurar que solo personal autorizado pueda realizar modificaciones o revisiones del código[1].

- Los repositorios fuentes de los sistemas de información no deberán estar contenidos en el ambiente de producción, sino en la herramienta de versionamiento definida por la OAPTI.

  - Prevención de Cambios No Autorizados: Se deben establecer procedimientos claros para prevenir la introducción de cambios no autorizados en el código fuente. Esto incluye un proceso de revisión y aprobación antes de que cualquier modificación sea implementada, asegurando que los cambios sean consistentes con los estándares de seguridad y calidad establecidos por la entidad.

Criptografía

10.29 Control SGSI-A.10.1.1 – A.10.1.2 - Política sobre el uso de controles criptográficos y gestión de llaves

Dictar lineamientos para el uso adecuado de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información del IDARTES, así mismo implementar el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

Lineamientos Generales:

La OAPTI establece los lineamientos para los controles criptográficos teniendo en cuenta lo siguiente, se deberán utilizar controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la información digital o electrónica reservada.

- Deberá verificar que todo sistema de información que requiera realizar transmisión de información clasificada como reservada cuente con mecanismos de cifrado de datos.
- Deberá desarrollar, establecer e implementar estándares para la aplicación de controles criptográficos.

- Deberá utilizar controles criptográficos para la transmisión de información clasificada, fuera del ámbito del IDARTES. La OAPTI deberán asegurarse de que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por los entes rectores de tecnología.
- La OPTI deberá disponer de herramientas que permitan el cifrado de medios de almacenamiento de información.
- Realizar un inventario y revisión periódica de llaves criptográficas y certificados digitales actualizado (uso, protección y tiempo de vida).

Seguridad Física y del entorno

10.30 Control SGSI-A.11.1.1 Perímetro de seguridad física

Dictar lineamientos para el acceso físico no autorizado, pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica del IDARTES, daño e interferencia para la información que se encuentre dentro o fuera de las instalaciones de procesamiento de información.

Lineamientos Generales:

La OAPTI establece los lineamientos para los controles de perímetro de seguridad física teniendo en cuenta lo siguiente:

- El perímetro de las áreas que contienen la información y sus instalaciones de procesamiento sensible o crítico deberán estar protegidos de accesos no permitidos.
- Las puertas y ventanas de las áreas seguras deberán permanecer cerradas con llave cuando no hay supervisión o están desocupadas.
- Todos los puntos de acceso deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación.
- El perímetro de seguridad debe contar con vigilancia y debe ser monitoreado por el personal de vigilancia designado por el IDARTES.

10.31 Control SGSI A.11.1.2 – 11.1.3 Controles de acceso físicos Seguridad de oficinas, recintos e instalaciones

Dictar lineamientos para proteger a través de controles de acceso para que solo se permita el ingreso a personal autorizado a las áreas seguras.

Lineamientos Generales:

- La Subdirección Administrativa y Financiera deberá señalizar las áreas de acceso restringido.
- La Subdirección Administrativa y Financiera deberá establecer un sistema de control de acceso a las instalaciones del IDARTES, así como a las áreas demarcadas con acceso restringido dentro y fuera de las instalaciones principales de la Entidad.

- Las áreas de acceso restringido deben estar protegidas por los controles adecuados al ingreso a ellas.
- La OAPTI autorizará el ingreso a personal ajeno al IDARTES a los centros de cableado para fines laborales y se harán responsables de la estadía de estos durante el tiempo que permanezcan en las instalaciones brindándoles el correspondiente acompañamiento.
- Todo el personal que ingrese al Centro de Datos y centros de cableado deberá portar identificación visible y presentarla en la puerta de acceso antes de su ingreso, como también registrarse en la bitácora digital de ingreso.
- La OAPTI deberán controlar que los centros de cableado permanezcan siempre con las puertas de acceso cerradas y con controles de seguridad que mitiguen el acceso a personal no autorizado.
- La OAPTI será responsable de la identificación y organización del cableado estructurado desde los puestos de trabajo hasta los paneles de conexión (patch panel) de los centros de cableado en las sedes.
- La Subdirección Administrativa y Financiera deberá mantener en buen estado la infraestructura física de los centros de cableado de todas las sedes y centro de datos de la sede principal, tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros.
- La OAPTI y la Subdirección Administrativa y Financiera deberán realizar una revisión periódica del estado de los centros de cableado e informar cualquier anomalía presentada de la siguiente manera:
  - Daños en el rack y equipos activos de red a la OAPTI
  - Daños en infraestructura física (puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros) a la Subdirección Administrativa y Financiera en las sedes de las localidades y en la sede principal del IDARTES.
- La Subdirección Administrativa y Financiera será responsable del cumplimiento del protocolo de aseo en los centros de cableado y centro de datos, este último contará con el acompañamiento de la OAPTI.
- La OAPTI será responsable de mantener organizado e identificado el cableado en los racks de los centros cableado y centro de datos.
- Se deberá establecer un plan de mantenimiento para los centros de cableado por parte de la OAPTI, de tal manera que se corrijan fallas y/o establecer mejoras en los mismos.
- La Subdirección Administrativa y Financiera, será responsable de la identificación y señalización necesaria de los centros de cableado y centro de datos.
- La Subdirección Administrativa y Financiera y la OAPTI, deberán mantener libre de objetos o elementos que no sean propios en la operación en el centro de datos y centros de cableado.
- La Subdirección Administrativa y Financiera deberá controlar y monitorear el ingreso a las áreas seguras.

10.32 Control SGSI-A.11.1.4 Protección contra amenazas externas y ambientales

Dictar lineamientos para diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

Lineamiento General:

- La OAPTI establecerá los lineamientos para los controles contra amenazas externas y ambientales y quedarán enmarcadas en los planes de contingencia, de emergencia y de continuidad de la operación.
- La OAPTI deberá monitorear las variables de temperatura y humedad de los centros de cableado o data center y, cuando estos se vean afectados por daño o falta de mantenimiento, se deberá reportar a la Subdirección Administrativa y Financiera dichas eventualidades para que estos equipos sean cambiados o se haga el mantenimiento necesario para su debido funcionamiento.

10.33 Control SGSI-A.11.1.5 Trabajo en áreas seguras

Dictar lineamientos para trabajar en áreas seguras.

Lineamientos Generales:

La Subdirección Administrativa y Financiera o a quien delegue deberá:

- Realizar revisiones periódicas de las oficinas que estén vacías asegurando que estén cerradas con llave.
- El trabajo en áreas seguras debe estar monitoreado, teniendo en cuenta que las cámaras no podrán apuntar directamente a la captura de información dentro de estas áreas.

10.34 Control SGSI-A.11.1.6 Áreas de despacho y carga

Dictar lineamientos para controlar los puntos de acceso tales como áreas de despacho y de carga, así como otros puntos donde pueda entrar personal no autorizado.

Lineamientos Generales:

La Subdirección Administrativa y Financiera o a quien delegue establece los lineamientos para los controles de área de despacho y carga teniendo en cuenta lo siguiente:

- Las áreas de cargue y descargue deberán estar señalizadas.
- Los puntos de acceso como el área de entrega y las zonas de carga deberán ser controladas y monitoreadas mediante CCTV.
- El material que ingresa se deberá inspeccionar y examinar para determinar la presencia de materiales peligrosos.

10.35 Control SGSI-A.11.2.1 Ubicación y protección de los equipos

Dictar lineamientos para la protección de la información en los equipos.

Lineamientos Generales:

La OAPTI y la Subdirección Administrativa y Financiera y Financiera establece los lineamientos para los controles de ubicación y protección de los equipos teniendo en cuenta lo siguiente:

- Los equipos de cómputo e impresoras deberán estar situados y protegidos para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.
- Los equipos de cómputo portátiles se deberán proteger mediante mecanismos que no permitan su pérdida.

10.36 Control SGSI-A.11.2.2 Servicio de suministro

Dictar lineamientos para la protección de los equipos de cómputo y procesamiento contra fallas de energía u otras interrupciones causadas por fallas en los servicios de suministro.

Lineamientos Generales:

- La OAPTI establece los lineamientos para el uso de la red de energía regulada en los puestos de trabajo en los cuales solo se deberán conectar equipos como computadores de escritorio, portátiles y pantallas; los otros elementos deberán conectarse a la red eléctrica no regulada.
- La OAPTI con el acompañamiento de la Subdirección Administrativa y Financiera deberán implementar mecanismos para regular el flujo de energía e interrupciones causadas por fallas en el soporte de los servicios públicos que puedan afectar los equipos de cómputo y procesamiento.
- La Subdirección Administrativa y Financiera deberá suministrar plantas eléctricas y UPS a las sedes del IDARTES, y garantizar su mantenimiento preventivo y correctivo.

10.37 Control SGSI-A.11.2.3 Seguridad en el Cableado

Dictar lineamientos para la protección de cableado de energía eléctrica y de telecomunicaciones contra interceptación, interferencia o daño.

Lineamientos Generales:

La OAPTI y la Subdirección Administrativa y Financiera definirán los controles de seguridad en el cableado teniendo en cuenta lo siguiente:

- El cableado que transporta datos y de suministro de energía deberán estar protegidos contra la interceptación, interferencia o daños.

- Los cables de energía eléctrica deberán estar separados de los cables de comunicaciones para evitar interferencias.
- Deberán tener en cuenta las consideraciones técnicas de las normas vigentes y las buenas prácticas.
- Los cuartos de cableado sólo podrán tener los elementos activos para su funcionamiento y no utilizarse como almacén para guardar cajas, mesas u otros equipos que no estén en uso.

10.38 Control SGSI-A.11.2.4 Mantenimiento de equipos

Dictar lineamientos para mantener correctamente los equipos para proteger su disponibilidad e integridad.

Lineamientos Generales:

La OAPTI establece los lineamientos para el mantenimiento de equipos teniendo en cuenta lo siguiente:

- Deberá definir mecanismos de soporte y mantenimiento a los equipos.
- Las actividades de mantenimiento tanto preventivo como correctivo deberán registrarse.
- Solo el personal autorizado deberá llevar a cabo el mantenimiento o las reparaciones a los equipos.
- Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deberán ser programadas.
- Los equipos que requieran salir de las instalaciones del IDARTES para reparación o mantenimiento deberán estar debidamente autorizados.
- Cuando un dispositivo vaya a ser reasignado o retirado de servicio, deberá garantizarse la eliminación de toda información siguiendo el Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo teniendo en cuenta que previo a esta actividad deberá realizar copia de seguridad de esta.

10.39 Control SGSI-A.11.2.5 Retiro de activos

Dictar lineamientos para no retirar de su sitio sin autorización previa los equipos, información o software.

Lineamientos Generales:

La Subdirección Administrativa y Financiera o su delegado establece los lineamientos para los controles de retiro de activos teniendo en cuenta lo siguiente:

- Se deberá registrar cuando los equipos de cómputo ingresan y se retiran de las instalaciones del IDARTES.
- Se deberá llevar un control en el almacén de los equipos cuando se asignan y cuando se hace su devolución.

10.40 Control SGSI-A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones

Dictar lineamientos para aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la entidad.

Lineamiento General:

- La OAPTI establece los lineamientos para que los equipos y medios retirados de las instalaciones no se dejen sin vigilancia en lugares públicos y se protejan adecuadamente.
- Deberá informar al jefe inmediato sobre la salida de los elementos de cómputo de las instalaciones del IDARTES.

10.41 Control SGSI-A.11.2.7 Disposición segura o reutilización de equipos

Dictar lineamientos para verificar que cualquier dato sensible o software licenciado haya sido retirado o sobrescrito en forma segura antes de la disposición o reúso del equipo.

Lineamientos Generales:

- Todos los equipos de cómputo que vayan a ser reasignados o dados de baja, se les deberá realizar una copia de respaldo y seguir el Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo.

10.42 Control SGSI-A.11.2.8 – A.11.2.9 Equipos de usuarios desatendidos Política de escritorio y pantalla limpia

Establecer mecanismos para reducir el riesgo contra pérdida, daño de información y el acceso no autorizado a los equipos del IDARTES, los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.

Lineamientos Generales:

La OAPTI establece los lineamientos para los equipos desatendidos y escritorio y pantalla limpia teniendo en cuenta lo siguiente, los funcionarios, funcionarias y/o contratistas deben seguir las siguientes directrices para proteger la información:

- Los colaboradores del IDARTES en el almacenamiento seguro de documentos y dispositivos, deben guardar en forma segura documentos y elementos de almacenamiento en (mis documentos del equipo, entre otros) especialmente cuando no se encuentren en sus sitios de trabajo. Esto ayuda a evitar accesos no autorizados, pérdida o daño de la información.
- Los colaboradores del IDARTES en la protección de Información en el Equipo de Cómputo, deben evitar guardar archivos que contengan información sensible o confidencial en el escritorio o en la pantalla inicial del computador. Estos archivos deben ser almacenados en rutas que dificulten el acceso a terceros, para prevenir fugas de información del IDARTES.
- Los colaboradores del IDARTES en el bloqueo de Sesión, deben tener en cuenta que es responsabilidad de los usuarios bloquear la sesión de usuario en el computador utilizando el protector de pantalla designado por la entidad, en los momentos en que no estén utilizando el equipo o cuando deban dejar su sitio de trabajo por cualquier motivo.

- Las contraseñas de los correos electrónicos institucionales estarán sincronizadas con las del usuario de red. Cada usuario debe mantener su contraseña segura y no compartirla, ya que es personal e intransferible.
- Los colaboradores del IDARTES, durante su ausencia no deberán conservar sobre el escritorio información propia del Instituto como: documentos físicos o medios de almacenamiento, por lo tanto, se requiere guardar en un lugar seguro para impedir su pérdida, daño, copia o acceso por parte terceros o personal que no tenga autorización para su uso o conocimiento.
- Los colaboradores del IDARTES, deberán bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el computador. El usuario debe bloquear su equipo usando las teclas: “Botón de windows + la tecla L” o “Ctrl + ALT+ SUPR + ENTER.
- Los colaboradores del IDARTES que impriman documentos con clasificación (Clasificada – Reservada), estos deberán ser retirados de la impresora inmediatamente y no se deberán dejar en el escritorio sin custodia.
- No se deberá reutilizar documentos impresos con clasificación (Clasificada – Reservada), estos deberán ser destruidos y no deberán estar como papel reciclable.
- Los documentos impresos con clasificación (Clasificada – Reservada) o que contenga datos personales no deberán publicarse.
- Los lugares de trabajo de los colaboradores del IDARTES y terceras partes que prestan sus servicios al Instituto y cuyas funciones no obliguen a la atención directa de ciudadanos deberán localizarse preferiblemente en ubicaciones físicas que no queden expuestas al público para minimizar los riesgos asociados al acceso no autorizado de la información o a los equipos informáticos.
- Todos los computadores del IDARTES deberán tener configurado y en operación un protector de pantalla con tiempo máximo de tres (3) minutos para que se active cuando el equipo no esté en uso.
- Todos los servidores públicos y contratistas de la Entidad deben conservar su escritorio libre de información propiedad de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento.
- No se debe consumir comidas o bebidas en el puesto de trabajo.

10.43 Control SGSI-A.12.1.1 Procedimientos de Operación Documentados

Dictar lineamientos para documentar los procedimientos de operación de la OAPTI del IDARTES.

Lineamientos Generales:

- La OAPTI deberá documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.
- Poner a disposición de todos los colaboradores los procedimientos de operación.
- Todos los desarrollos y acciones en la infraestructura TI deben estar soportadas documentalmente.

10.44 Control SGSI-A.12.1.2 Gestión de cambios

Dictar lineamientos para controlar y reducir al mínimo el impacto sobre los cambios normales y de emergencia que se generen sobre los servicios, infraestructura y aplicativos de TI administrados por la OAPTI del IDARTES.

Lineamientos Generales:

- La OAPTI establece un procedimiento que permita asegurar la gestión de cambios normales y de emergencia a nivel de infraestructura, aplicativos y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficiencia, seguridad, calidad y permitan determinar los responsables y tareas en la gestión de cambios.
- Establecer un comité de cambios, quien se encargará de evaluar, aprobar o negar la implementación de los cambios y este a su vez será presidido por un Gestor de Cambios del Operador TI. Este comité deberá estar conformado por tres integrantes del IDARTES de OAPTI.

10.45 Control SGSI-A.12.1.3 Gestión de capacidad

Dictar lineamientos para hacer el seguimiento al uso de recursos tecnológicos, para realizar ajustes y proyecciones de requisitos de capacidad futura de los servicios e infraestructura de tecnología del IDARTES.

Lineamientos Generales:

La OAPTI deberá documentar una gestión de capacidad la cual le permita:

- Evaluar las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.
- Monitorear el rendimiento de la infraestructura tecnológica para determinar el uso de la capacidad existente.
- Documentar los datos de rendimiento y capacidad de la plataforma tecnológica del IDARTES.
- Documentar los acuerdos de niveles de servicio.
- Asignar los recursos adecuados de hardware y software, para todos los servicios y aplicaciones de tecnología.
- Documentar una gestión de capacidad, las recomendaciones de mejora de la infraestructura de tecnología y periódicamente deberá ser actualizado.

10.46 Control SGSI-A.12.1.4 Separación de los ambientes de desarrollo, pruebas y producción

Dictar lineamientos para realizar la separación de los ambientes de desarrollo, pruebas y producción con los que cuenta el IDARTES y de esta manera reducir los riesgos de cambios no autorizados.

Lineamientos Generales:

La OAPTI deberá:

- Realizar la separación de ambientes de desarrollo, pruebas y producción, los cuales deberán estar separados de manera física y lógica.
- Definir y documentar los lineamientos a seguir para la transferencia entre ambientes.
- Utilizar datos que no sean sensibles para el IDARTES en los ambientes de prueba, exceptuando aquellos casos en los que el usuario funcional solicita la restauración de datos de producción para verificar la correcta funcionalidad.
- Permitir que los ambientes de prueba, desarrollo y producción sean similares para prevenir situaciones en las cuales el software desarrollado presente comportamientos distintos y errores.
- Utilizar nombres de dominios diferentes para los ambientes de prueba, desarrollo y producción para evitar confusión y diferenciar de manera clara cada ambiente.
- Garantizar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y nunca en los ambientes de pruebas o producción.

10.47 Control SGSI-A.12.2.1 Controles contra códigos maliciosos

Implementar controles de detección, prevención y recuperación, así como sensibilizar a los colaboradores del IDARTES para la protección contra códigos maliciosos.

Lineamientos Generales:

La OAPTI deberá:

- Definir y documentar los controles para la detección, prevención y recuperación contra códigos maliciosos.
- Realizar campañas de concienciación de usuarios en materia de protección, prevención y recuperación contra códigos maliciosos.
- Dictar los lineamientos para la instalación de software antivirus que brinde protección contra códigos maliciosos en todos los recursos informáticos del IDARTES y asegurar que estas herramientas no puedan ser deshabilitadas, así como mantenerlas actualizadas permanentemente.
- Realizar la actualización continua de la base de firmas y parches correspondiente del software de Antivirus y actualizaciones de sistema operativo.
- Todo mensaje sospechoso de procedencia desconocida deberá ser inmediatamente reportado a la OAPTI a través de la mesa de servicio, tomando las medidas de control necesarias.

10.48 Control SGSI-A.12.3.1 Respaldo de la información

Dictar lineamientos para establecer un esquema de copias de seguridad, mediante estrategias orientadas a la protección de la información.

Lineamientos Generales:

- La OAPTI deberá realizar y mantener copias de seguridad de la información digital solicitadas por el líder funcional o líder técnico.
- La OAPTI deberá documentar un lineamiento de copia de seguridad del IDARTES donde se establezca esquemas de: qué, cuándo, con qué periodicidad y cuál es la criticidad para realizar las copias de respaldo de información.
- En cualquier momento la OAPTI, podrá realizar copias de información de colaboradores, producto de solicitudes que provengan de los directores, supervisores de contrato o jefes de oficina.
- La OAPTI deberá definir la custodia y almacenamiento de las copias.
- La OAPTI deberá tener un inventario y bitácora de las copias que se realizan y de las copias que se restauran.
- La OAPTI deberá dar los lineamientos para la realización de las copias de seguridad conforme al procedimiento respaldos y retenciones establecido.
- La OAPTI deberá establecer los lineamientos y directrices para el respaldo de copias de las aplicaciones descentralizadas que se encuentran en las sedes del IDARTES.
- Con el fin de garantizar una gestión eficiente de las copias de seguridad y evitar el almacenamiento innecesario de datos obsoletos, la OAPTI establece que las copias de seguridad con una antigüedad superior a cinco (5) años deberán ser eliminadas.
- Al cierre de la relación contractual, el contratista deberá transferir y almacenar en el repositorio designado (NAS) la información (registros, fotografías, documentos, imágenes, etc.) de gestión del área, como requisito para la emisión del paz y salvo. El supervisor del contrato será responsable de verificar la correcta transferencia, integridad y disponibilidad de la información, así como de asegurar que esta se encuentre sujeta a las políticas institucionales de respaldo y conservación.

10.49 Control SGSI-A.12.4 Registro (Logging) y Seguimiento

Dictar lineamientos que permitan registrar los eventos y evidencias, que los usuarios y administradores realizan en los sistemas de información e infraestructura tecnológica.

Lineamientos Generales:

- La OAPTI deberá generar registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren.
- La OAPTI deberá salvaguardar los registros de auditoría que se generen de cada sistema.

- La OAPTI deberá monitorear excepciones o los eventos de la seguridad de información.
- La OAPTI deberá monitorear la infraestructura tecnológica para verificar que los usuarios sólo la usen para actividades propias de su labor y la Misión del IDARTES.
- La OAPTI deberá sincronizar los relojes de los servidores con una única fuente de referencia de tiempo (http://horalegal.inm.gov.co/), con el fin de garantizar la exactitud de los registros de auditoría.

10.50 Control SGSI-A.12.5 Instalación de software en sistemas operativos

Dictar lineamientos que permitan controlar la instalación de software en sistemas operativos propiedad del IDARTES.

Lineamientos Generales:

- La OAPTI deberá controlar y tener registros de la actualización del software en producción, aplicaciones y librerías de programas propios del IDARTES.
- La OAPTI deberá usar controles para proteger todo el software implementado y la documentación del sistema.
- La OAPTI deberá conservar las versiones anteriores del software de aplicación como una medida de contingencia.

10.51 Control SGSI-A.12.6.1 Gestión de vulnerabilidad técnica

Dictar lineamientos para revisar de manera periódica las vulnerabilidades técnicas de los sistemas de información críticos y misionales.

Lineamientos Generales:

- La OAPTI deberá realizar de manera periódica revisión de vulnerabilidades técnicas por medio de pruebas de penetración, a la plataforma tecnológica de la entidad.
- La OAPTI deberá documentar, informar, gestionar y corregirlos hallazgos de las vulnerabilidades adoptando las acciones preventivas y correctivas necesarias para minimizar el nivel de riesgo y reducir el impacto.
- La OAPTI deberá definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, las pruebas de gestión, la aplicación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.
- Todo análisis de vulnerabilidad o prueba de penetración debe contar con la autorización del Jefe de OAPTI o, a quien este delegue y estas deberán ser previamente informadas a las partes interesadas con el fin de evaluar el riesgo de la ejecución de ellas, su alcance y el cumplimiento de la normatividad vigente.

10.52 Control SGSI-A.12.6.2 Restricciones sobre la instalación de Software

Dictar lineamientos para las restricciones sobre la instalación de Software.

Lineamientos Generales:

- La OAPTI deberá monitorear que la Infraestructura tecnológica del IDARTES no sea utilizada para actividades comerciales o para propósitos de entretenimiento, acceso o uso a material no autorizado.
- La OAPTI deberá establecer que la infraestructura tecnológica sea usada exclusivamente para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas.
- La OAPTI deberá controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada y no viole derechos de autor.
- La OAPTI podrá en cualquier momento realizar una inspección del software instalado en los equipos de cómputo.
- La OAPTI designará y autorizará al personal para instalar, configurar y dar soporte a los equipos de cómputo del IDARTES.
- Sólo está permitido el uso de software licenciado por el IDARTES y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado por la OAPTI.
- Las aplicaciones generadas por el IDARTES, en desarrollo de su misión institucional, deberán ser reportadas y gestionadas con los lineamientos definidos con la OAPTI.
- La OAPTI es la única dependencia autorizada para la administración del software, el cual no deberá ser copiado, suministrado a terceros o utilizado para fines personales.

10.53 Control SGSI-A.12.7 Consideraciones sobre auditorias de sistemas de información

Dictar lineamientos para revisar y auditar periódicamente los sistemas de información del IDARTES.

Lineamientos Generales:

- La OAPTI deberá planificar actividades que involucren auditorias de los sistemas críticos en producción, limitando el acceso al sistema de información y a los datos de solo de lectura (en caso de acceso diferente al de solo lectura se deberá acordar previamente), determinando tareas, responsables y estas se deberán realizar fuera del horario laboral.
- La OAPTI deberá definir y gestionar los planes de mejoramiento que se generan de los resultados de las auditorias de los sistemas de Información del IDARTES.

Seguridad de las Comunicaciones

10.54 Control SGSI A.13.1 Gestión de la Seguridad de las redes

Dictar lineamientos para la protección de la información en las redes y sus instalaciones de procesamiento de información.

Lineamientos Generales:

- La OAPTI deberá proporcionar una plataforma Tecnológica que soporte los sistemas de información, esta deberá estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes de terceros y del servicio de acceso a internet. La división de estos segmentos deberá ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad.
- La OAPTI deberá realizar segmentación de redes para colaboradores y visitantes del IDARTES.
- La OAPTI deberá establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
- La OAPTI deberá garantizar que los puertos físicos y lógicos de diagnósticos y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.
- La OAPTI deberá establecer la documentación necesaria para la utilización de los servicios de red restringiendo el acceso a los servicios de red y a las aplicaciones.
- La OAPTI deberá realizar revisiones y monitoreo regularmente en la gestión de los servicios de manera segura y que se encuentran en los acuerdos de servicios de red establecidos con los proveedores y/o terceras partes del IDARTES.

10.55 Control SGSI-A.13.1.1 – SGSI-A.13.1.2 – SGSI-A.13.1.3 Controles de redes Seguridad de servicios de las aplicaciones en redes públicas protección de transacciones de los servicios de las aplicaciones

Dictar lineamientos para la protección de la información en las redes y sus instalaciones de procesamiento de información.

Lineamientos Generales:

- La OAPTI deberá definir controles para la transferencia de información a través de redes públicas para las aplicaciones del IDARTES.

La OAPTI deberá disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones del IDARTES, teniendo en cuenta los siguientes criterios:

- Contar con información de autenticación secreta de usuario.
- Usar firmas o certificados digitales en caso de ser necesario.
- Mantener protocolos seguros para la comunicación entre las partes.

- La OAPTI deberá cifrar las comunicaciones entre DMZ y los servidores de la red interna.
- Los protocolos de comunicación entre la red interna y la DMZ estén asegurados con el fin de prevenir fugas de información.
- La información almacenada de las transacciones no se encuentre pública.

La OAPTI deberá disponer de una zona desmilitarizada o DMZ, entre la red interna del IDARTES y la red externa (internet) con el objetivo de delimitar conexiones desde la red interna hacia Internet y limitar las conexiones desde Internet hacia la red interna del IDARTES con los siguientes criterios:

- El tráfico de la red externa a la DMZ está limitado.
- El tráfico de la red externa a la red interna deberá estar controlado.
- El tráfico de la red interna a la DMZ está limitado.
- El tráfico de la red interna a la red externa está autorizado.
- El tráfico de la DMZ a la red interna está prohibido.
- El tráfico de la DMZ a la red externa está denegado.

- La DMZ se deberá implementar para ofrecer servicios que necesitan acceso desde Internet. Estos servicios deberán ser monitoreados con el fin de prevenir ataques.
- La arquitectura de la DMZ deberá estar aislada de la red interna del IDARTES de forma que no permita el acceso no autorizado a la red interna, por lo que se deberán diseñar redes perimetrales con los siguientes objetivos:
  - No se pueden hacer consultas directas a la red interna del IDARTES desde redes externas e internet
  - Se deberá realizar la segmentación de redes y listas de acceso a los servicios del IDARTES tales como servidores, administración, invitados, Etc.
  - El acceso a la red de datos del IDARTES y a los sistemas de información soportados por la misma, es de carácter restringido. Se concederán permisos con base a “la necesidad de conocer” y el “acceso mínimo requerido” conforme a los criterios de seguridad de la información contemplados en la presente política.
  - La conexión a la red wifi institucional para funcionarios deberá ser administrada desde OAPTI mediante un SSID único, la autenticación deberá ser con usuario y contraseña de directorio activo.
  - La conexión a la red wifi institucional para visitantes deberá tener un SSID y contraseñas diferentes para cada sede administrativa, administrada por la OAPTI, No se podrá conectar dispositivos móviles personales a la red wifi, salvo los de la Oficina Asesora de Comunicaciones, Dirección General y los aprobados por la OAPTI a través de una solicitud a la mesa de servicio.

10.56 Control SGSI-A.13.2.1 -A.13.2 2 Políticas y Procedimientos de Transferencia de información Acuerdos sobre transferencia de información

Dictar lineamientos de seguridad para la información transferida dentro del IDARTES con cualquier entidad externa.

Lineamientos Generales:

- Los Colaboradores de IDARTES o terceros que necesiten transferir información sensible (ya sea pública clasificada o pública reservada) deben firmar un “Acuerdo de Confidencialidad” que detalle las responsabilidades de cada parte y garantice la protección de la información. Además, es indispensable contar con la autorización previa de su superior inmediato.

- Todos los intercambios de información con entidades o partes externas, que no sean los entes de control, deben estar respaldados por contratos, convenios o acuerdos formalizados. Estos documentos deberán especificar los medios y controles para el manejo de la información. Además, es necesario firmar acuerdos de confidencialidad que aseguren la protección de la información tanto durante como después del período de vigencia de los compromisos. Estos acuerdos deben cumplir con la normativa vigente en materia de protección de datos, en particular con la Ley de Habeas Data (Ley 1266 de 2008 y sus decretos reglamentarios), la Ley de Protección de Datos Personales (Ley 1581 de 2012 y sus decretos reglamentarios), y la Ley de Transparencia (Ley 1712 de 2014 y sus decretos reglamentarios).
- La OAPTI deberá contar con los lineamientos para proteger la información transferida con respecto a la interceptación, copiado, modificación, enrutado y destrucción de esta.
- La OAPTI deberá establecer mecanismos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas.
- La OAPTI deberá establecer controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico del IDARTES.
- La OAPTI dictará directrices sobre retención, disposición y transferencia de la información del IDARTES, de acuerdo con la legislación y reglamentaciones locales y nacionales.
- La OAPTI deberá establecer un acuerdo para la transferencia de información entre el IDARTES y las partes externas.
- La OAPTI deberá definir lineamientos para la recolección de evidencias de elementos informáticos, con el fin de garantizar la autenticidad de los elementos materiales de prueba recolectados y examinados, asegurando que pertenecen al caso investigado, sin confusión, adulteración o sustracción.

11. Control SGSI-A.13.2.3 Mensajería electrónica

Proteger adecuadamente la información incluida en la mensajería electrónica.

Lineamientos Generales:

- La OAPTI deberá implementar controles para el direccionamiento y transporte correcto del mensaje, así como la confiabilidad y disponibilidad del servicio.
- La OAPTI otorgará la aprobación a los colaboradores o terceros que requieran usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información, estos serán monitoreados y revocados en caso de ser necesario.

11.1 Control SGSI-A.13.2.4 Acuerdos de confidencialidad o de no divulgación

- Identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la entidad para la protección de la información y de los datos personales de acuerdo a la normatividad vigente.

- Como parte de sus términos y condiciones iniciales de trabajo, los colaboradores, cualquiera sea su nivel jerárquico dentro del IDARTES, formalizaran un compromiso de confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del IDARTES.
- En el caso de que sea personal externo que ejecute tareas propias del IDARTES y haya sido contratado en el marco de un contrato o convenio con el IDARTES, deberá reposar en la carpeta de ejecución del contrato un compromiso de confidencialidad firmado por el Representante Legal.

Adquisición, desarrollo y mantenimiento de sistemas

11.2 Control SGSI-A.14.1.1 Análisis y especificación de requisitos de seguridad de la información

Dictar lineamientos que permitan incluir requisitos relacionados con seguridad de la información en nuevos sistemas de información y en las mejoras de los existentes.

Lineamientos Generales:

- La OAPTI deberá disponer de requerimientos para las solicitudes de nuevos sistemas de información y modificaciones a los existentes en el IDARTES que cuenten con el análisis e implementación de criterios de seguridad del software.
- La OAPTI deberá contar con los mecanismos para justificar, acordar y documentar en la fase de requisitos y en la fase de modificación de los sistemas del IDARTES, los criterios de seguridad de la información.
- La OAPTI deberá contar con los componentes de seguridad de la información para los siguientes criterios:
- El suministro de funcionalidades que permitan el acceso y la autorización para usuarios del IDARTES privilegiados, técnicos y usuarios finales.
- El suministro de funcionalidades que permitan al proceso o al usuario funcional la administración de los roles, permisos y acceso a la información de los sistemas de información.
- Informar a los usuarios finales sobre los mecanismos de uso y apropiación de los sistemas de información,
  a través de la documentación que soporta las aplicaciones.
  Proveer las aplicaciones definidas como críticas para la entidad con funcionalidades que cumplan los procesos como registro de transacciones, seguimiento y no repudio.

Para los procesos de interoperabilidad con otros sistemas externos se debe tener en cuenta los siguientes aspectos:

- Servicios web REST (Representational State Transfer): Utilizar métodos HTTP estándar (GET, POST, PUT, DELETE) para intercambiar datos de forma ligera, flexible y escalable.
- Asegurar el cumplimiento con normativas como protección de datos personales, propiedad intelectual.
- Asegurar que las integraciones externas siguen prácticas seguras de desarrollo.
- Definir protocolos seguros para el intercambio de datos (por ejemplo, cifrado en tránsito).

- Establecer acuerdos de confidencialidad con las partes involucradas en los procesos de interoperabilidad.

11.3 Control SGSI-A.14.2.1 Política de desarrollo seguro

Dictar lineamientos que permitan establecer reglas para el desarrollo de sistemas de información dentro del IDARTES.

Lineamientos Generales:

La OAPTI deberá establecer los mecanismos necesarios para la creación de software, teniendo en cuenta los siguientes aspectos:

- Orientar sobre buenas prácticas de seguridad en el desarrollo del software.
- Requisitos de seguridad en el control de versiones.
- Capacidad de los desarrolladores para evitar, encontrar y resolver vulnerabilidades.
- Establecer las condiciones para garantizar que todo el ciclo de desarrollo de software sea realizado bajo condiciones de seguridad y en ambientes controlados, que minimicen la posibilidad de materialización de riesgos que afecten la información.
- La OAPTI deberá tener en cuenta el punto anterior para la reutilización de códigos.
- La OAPTI deberá proteger los códigos ejecutables y código de desarrollo o compiladores del software operacional y aplicaciones propios del IDARTES.
- Se deben seguir técnicas de programación seguras y buenas prácticas de seguridad de la información para el desarrollo de sistemas de información, por ejemplo, las recomendadas por OWASP (Proyecto Abierto de Seguridad en Aplicaciones WEB).
- Para el desarrollo contratado externamente, es necesario que el tercero cumpla con los lineamientos de desarrollo seguro que establezca la OAPTI del IDARTES.

11.4 Control SGSI-A.14.2.2 - SGSI-A.14.2.3 - SGSI-A.14.2.4 Procedimientos de control de cambios en sistemas - Revisión técnica de las aplicaciones después de cambios en la plataforma de operación - Restricciones en los cambios a los paquetes de software

Dictar lineamientos que permitan establecer procedimientos y revisión de los cambios de las aplicaciones críticas del IDARTES y desalentar los cambios en los paquetes de estos.

Lineamientos Generales:

- La OAPTI deberá definir controles para que los cambios de los Sistemas de Información en el IDARTES sean documentados, teniendo en cuenta la integridad de los sistemas desde las primeras etapas de diseño y a través de los mantenimientos posteriores.
- La OAPTI deberá definir un proceso formal para el desarrollo, mantenimiento, inclusión y cambios importantes de los sistemas de información involucrando pruebas, control de calidad e implementación.

- La OAPTI deberá definir para los cambios en los sistemas del IDARTES los siguientes aspectos:
  - Niveles de autorización acordados.
  - Presentar los cambios a los usuarios autorizados.
  - Revisar la integridad para asegurar que no se vean comprometidos los cambios.
  - Identificar y validar el código para minimizar la posibilidad de existencia de vulnerabilidades conocidas.
- Antes de cualquier cambio, hay que asegurar que los usuarios autorizados aceptan los cambios.
- Mantener un control de versiones para las actualizaciones de los sistemas.
- Mantener un rastro de auditoría de los cambios.
- Asegurar que los cambios se hagan en momentos adecuados y que no afecten los procesos del IDARTES.
- La OAPTI deberá guardar en un repositorio, las versiones anteriores de cada sistema de información que esté actualizado.
- La OAPTI deberá definir la manera de revisar después de un cambio importante que el sistema de información alterado no se haya comprometido.
- La OAPTI deberá definir la manera para notificar a tiempo los cambios de los sistemas, permitiendo realizar pruebas y revisiones apropiadas antes de su implementación.
- La OAPTI deberá evitar las modificaciones a los paquetes de software, en la medida de lo posible se deberán usar directamente los dados por el proveedor; limitándose únicamente a cambios necesarios, cuando se hagan, se deberán tener en cuenta los siguientes aspectos:
  - El riesgo en que se puede ver involucrado el sistema de información.
  - Verificar si se requiere consentimiento del usuario funcional.
  - Verificar la posibilidad que el proveedor realice dichos cambios.
  - La compatibilidad con otro software en uso.
- La OAPTI deberá conservar el software original cuando se hayan realizado cambios en los paquetes de este.
- Toda actividad del ciclo de desarrollo debe contar con la respectiva documentación técnica y administrativa conforme a los lineamientos para desarrollo definidos y alineados con MINTIC.

11.5 Control SGSI-A.14.2.5 – SGSI-A.14.2.6 Principios de construcción de sistemas seguros Ambiente de desarrollo Seguro

Dictar lineamientos que permitan establecer reglas para los principios de desarrollo de sistemas de información seguros dentro del IDARTES, igualmente contar con ambientes de desarrollo seguros para todo el ciclo de vida de los sistemas.

Lineamientos Generales:

- La OAPTI deberá aplicar en los desarrollos de sistemas de información los principios y buenas prácticas de seguridad de la información.

- La OAPTI deberá acatar las recomendaciones que se realicen los entes rectores en materia de Seguridad de la Información para el desarrollo seguro de sistemas de la información.
- La OAPTI deberá definir ambientes de desarrollo seguro, teniendo en cuenta los siguientes aspectos:
  - El carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir.
  - Requisitos externos como reglamentaciones o políticas.
  - Controles de Seguridad ya establecidos por el IDARTES.
  - Separación entre diferentes ambientes de desarrollo.
  - Control de acceso al ambiente de desarrollo.
- Seguimiento de los cambios en el ambiente y los códigos almacenados allí.
- Control sobre el movimiento de datos desde y hacia el ambiente.

11.6 Control SGSI-A.14.2.7 Desarrollo contratado externamente

Dictar lineamientos que permitan establecer reglas para realizar seguimiento a los desarrollos de sistemas de información contratados externamente para funcionamiento dentro del IDARTES.

Lineamientos Generales

La OAPTI deberá definir controles para que los sistemas adquiridos externamente cumplan con los siguientes aspectos:

- Acuerdos de licenciamiento, propiedad de códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente.
- Requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.
- Establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
- Realizar pruebas para vigilar que no exista contenido malicioso intencional y no intencional en el momento de la entrega.

11.7 Control SGSI-A.14.2.8 – SGSI-A.14.2.9 Pruebas de seguridad de sistemas - Prueba de aceptación de sistemas

Dictar lineamientos que permitan establecer pruebas de seguridad y de aceptación de los sistemas del IDARTES.

Lineamientos Generales:

- La OAPTI deberá contemplar en los cambios y en los nuevos sistemas de información, pruebas de aceptación asociadas a los requisitos de seguridad de la información.

11.8 Control SGSI-A.14.3.1 Protección de datos de Prueba

Dictar lineamientos que permitan establecer reglas para la protección de datos de pruebas de los Sistemas de Información del IDARTES.

Lineamientos Generales:

- La OAPTI deberá evitar durante la ejecución de pruebas en ambientes de desarrollo el uso de datos que contengan información personal o información sensible del IDARTES que este contenida en el ambiente de producción de las aplicaciones, exceptuando aquellos casos en los que el usuario funcional solicita la restauración de datos de producción para verificar la correcta funcionalidad.
- La OAPTI deberá tener en cuenta controles de acceso a los ambientes de producción y de prueba.

Relación con Proveedores

11.9 Control SGSI-A.15 Seguridad de la información para las relaciones con proveedores - Tratamiento de la seguridad dentro de los acuerdos con proveedores - Cadena de suministro de tecnología de información - Seguimiento y revisión de los servicios de los proveedores

Dar los lineamientos de seguridad de la información para las relaciones con proveedores que trabajen con el IDARTES.

Lineamientos Generales:

- La OAPTI deberá establecer lineamientos para el cumplimiento de las obligaciones contractuales de la estrategia de Seguridad de la Información con terceros o proveedores.
- La OAPTI deberá establecer en el momento de suscribirse contratos de apoyo a la gestión que se desarrollen dentro del IDARTES, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información del IDARTES.
- La OAPTI deberá dar lineamientos técnicos para establecer en los contratos con terceros y proveedores teniendo en cuenta los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
- La OAPTI deberá documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica del IDARTES.
- La OAPTI deberá verificar mensualmente el cumplimiento de Acuerdos de Nivel de Servicio – OLA, establecidos con sus proveedores de tecnología.
- La OAPTI deberá establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en la gestión de cambios.

- Cada dependencia del IDARTES que establezca relación con proveedores y su cadena de suministro, solicitará capacitación periódica de Seguridad de la Información con el fin de dar a conocer las políticas que tiene el IDARTES.

Gestión de Incidentes de Seguridad de la Información

11.10 Control SGSI-A.16.1.1 – A.16.1.7 Responsabilidad y procedimientos - Reporte de eventos de seguridad de la información - Reporte de debilidades de seguridad de la información - Evaluación de eventos de seguridad de la información y decisiones sobre ellos - Respuesta a incidentes de seguridad de la información - Aprendizaje obtenido de los incidentes de seguridad de la información - Recolección de evidencia

Dictar lineamientos que permitan asegurar al IDARTES un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Lineamientos Generales:

- La OAPTI deberá definir los lineamientos para:
  - Responsables de la gestión de incidentes de seguridad de la información.
  - Los canales para que los colaboradores del IDARTES puedan reportar los incidentes de seguridad de la información.
  - Para la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos.
  - Para la recolección de evidencia de incidentes de seguridad de la información.
- La OAPTI deberá contar con los mecanismos para el cumplimiento de los tiempos en la respuesta de incidentes, establecido en los lineamientos para la gestión de Incidentes.
- La OAPTI deberá proporcionar los medios para el aprendizaje al IDARTES de los incidentes de seguridad de la información.
- La OAPTI deberá dar a conocer a los colaboradores del IDARTES los lineamientos establecidos para la gestión de incidentes de seguridad de la información.

Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocio

11.11 Control SGSI A.17.1.1 Planificación de la continuidad de la seguridad de la información

La OAPTI deberá establecer el plan de recuperación de desastres tecnológicos de la Entidad, por medio del cual se continúe brindando el servicio durante una emergencia o desastre, y restaure los servicios críticos de tecnología identificados.

Lineamientos Generales:

- Se deben identificar y documentar los requisitos de seguridad de la información en cada una de las estrategias de recuperación de desastres identificadas en la Entidad.

11.12 Control SGSI-A.17.1.2 Implementación de la continuidad de la seguridad de la información

Esta política pretende establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

Lineamientos Generales:

- Se deberán conformar los equipos de respuesta ante incidentes de seguridad de la información.
- El IDARTES deberá elaborar un plan de recuperación de desastres tecnológicos para los servicios misionales críticos que se apoyan en las TIC para su funcionamiento identificados en el análisis de impacto al negocio.
- En caso de presentarse un incidente de seguridad de la información significativo se deberá gestionar el manejo de la crisis y los mecanismos de comunicación apropiados tanto internos como externos durante el estado de contingencia.
- La OAPTI deberá documentar los procedimientos, guías o instructivos para configurar los servicios de TIC identificados en el análisis de impacto al negocio durante situaciones adversas.

11.13 Control SGSI-A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Verificar que las pruebas realizadas sean consistentes con el alcance y el objetivo del Plan de Continuidad TI y minimicen la interrupción de las operaciones.

Lineamientos Generales:

- La OAPTI deberá verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
- Se debe definir un equipo para la planeación de pruebas, los procesos que estarán involucrados, la infraestructura tecnológica y/u operativa requerida, el plan de rollback y las actividades a realizar.
- Los participantes de los equipos deberán recibir sensibilización con respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.
- Para el Plan de continuidad TI se deberá establecer un programa de pruebas, teniendo en cuenta los requerimientos técnicos necesarios.
- Las pruebas deberán ejecutarse de manera que simule las condiciones de un evento y no se afecte la operación.

- Se deben documentar las pruebas y se deben generar reportes o informes después de cada prueba y/o ejercicio que incluya recomendaciones, lecciones aprendidas y acciones para mejorar el plan.
- Se deberá contar con planes de contingencia de los servicios de tecnología.
- Se deben ejecutar procedimientos de control de cambios según las acciones preventivas y correctivas que se generaron a partir de las pruebas, para asegurar que los planes de recuperación de desastres tecnológicos se mantengan actualizados.
- La OAPTI deberá revisar y aprobar el plan de recuperación de desastres tecnológicos.

11.14 Control SGSI A.17.2.1 Disponibilidad de instalaciones de procesamiento de información

Disponer de las instalaciones de procesamiento de información requeridas en el plan de recuperación de desastres tecnológicos.

Lineamientos Generales:

- Deberá implementar redundancia suficiente, para lo cual deberá considerar componentes o arquitecturas redundantes.
- Deberá poner a prueba los componentes o arquitecturas redundantes implementadas para asegurar que después de una falla el componente funcione.

Cumplimiento

11.15 Control SGSI-A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Dictar lineamientos para cumplir con los requisitos de legislación y regulación externa e interna del IDARTES.

Lineamientos Generales:

- La OAPTI a través de la estrategia de Seguridad de la Información deberá identificar, documentar y actualizar todos los requerimientos contractuales, estatutarios y reglamentarios con el fin de salvaguardar la información de la entidad dar cumplimiento a la normatividad vigente utilizando la herramienta de verificación de requisitos legales.
- La Oficina Jurídica deberá asesorar al MSPI de Seguridad de la Información en la documentación técnica y administrativa con el fin de incorporar un marco legal a la gestión TI.

11.16 Control SGSI-A.18.1.2 Derechos de propiedad Intelectual

Dictar lineamientos para cumplir con los requisitos legislativos, reglamentarios y contractuales acerca del uso de software patentado y material con respecto al cual pueden existir derechos de propiedad intelectual.

Lineamientos Generales:

- La OAPTI deberá definir controles con el objetivo de proteger adecuadamente la propiedad intelectual del IDARTES, tanto propia como la de terceros, tales como derechos de autor de software, licencias y código fuente. El material registrado con derechos de autor no se deberá copiar sin la autorización del propietario.
- La OAPTI deberá a través del MSPI de Seguridad de la Información deberá generar conciencia a los colaboradores del IDARTES sobre los derechos de propiedad intelectual y la protección de datos.

11.17 Control SGSI A.18.1. 3 - SGSI A.18.1.5 Protección de Registros - Reglamentación de controles criptográficos

Dictar lineamientos para cumplir con la protección de registros contra pérdida, destrucción y falsificación aplicando los requisitos legislativos, reglamentarios, contractuales y del IDARTES.

Lineamientos Generales:

- La OAPTI con apoyo de Gestión Documental, deberán definir y establecer:
  - Directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información física y digital.
  - Deberá establecer e implementar controles para proteger los registros en su confidencialidad, integridad y disponibilidad.
  - Deberá establecer procedimientos de almacenamiento a largo plazo y manipulación de los registros físicos y digitales.
- La OAPTI, deberá identificar, gestionar y documental los controles criptográficos necesarios en la infraestructura tecnológica del IDARTES.

11.18 Control SGSI A.18.1.4 Privacidad y protección de información de datos personales

Dictar lineamientos para cumplir con la protección de datos personales.

- La OAPTI y la OJ, deberán definir una política de tratamiento de datos personales, para la protección de los derechos fundamentales en su tratamiento y todos los procesos asociados a esta y toda la documentación que esta amerite.

11.19 Control SGSI A.18.2 Revisión independiente de la seguridad de la información - Cumplimiento con las políticas y normas de seguridad - Revisión del cumplimiento técnico

Dictar lineamientos para asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos del IDARTES.

Lineamientos Generales:

- La Oficina de Control Interno, deberá realizar auditorías internas para comprobar el correcto funcionamiento del Modelo de Seguridad de la Información en cuanto a los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información.
- Los líderes de los procesos deberán asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas.
- Cada usuario debe asumir su responsabilidad respecto a los riesgos en seguridad de la información y la protección de los activos de información del IDARTES.
- El incumplimiento a la Política Digital, Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a Seguridad y Privacidad de la Información se refiere, en especial sanciones disciplinarias de conformidad con la Ley 734 de 2002 "Código Disciplinario Único".

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS
1	2014-01-01	Emisión inicial
2	2015-09-01	Se ajustan los manejos de las contraseñas y actualización del servicio de correo bajo la plataforma Google
3	2017-01-02	Se realizan cambios en seguridad de las cuentas de correo y drive, se eliminan servicios obsoletos, se incluyen las políticas de gestión de activos y se incluyen políticas de copia y seguridad de la información.
4	2021-09-20	Actualización de todos los capítulos de la política de acuerdo con la nueva normatividad establecida
5	2023-12-07	Actualización de nombre y contenido de las políticas de acuerdo con la nueva normatividad establecida.
6	2024-09-24	Actualización del nombre y contenido de las políticas de seguridad, se incluye el cumplimiento de la política de seguridad digital, acorde a la Resolución 0500 de 2021 del MINTIC. Esta actualización abarca la protección de los sistemas, redes, aplicaciones, dispositivos y demás activos digitales utilizados en la Entidad.
7	2025-06-20	El documento ha sido actualizado con el objetivo de fortalecer y optimizar las políticas operativas relacionadas con la gestión de copiado, restauración y depuración de respaldos (backups) de la información del usuario final. Esta actualización busca asegurar la disponibilidad, integridad y trazabilidad de los datos, en concordancia con las buenas prácticas de seguridad de la información y las directrices institucionales vigentes. Adicionalmente, se realizaron ajustes relacionados con la definición de roles, asignación de responsabilidades y mecanismos de seguimiento dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

CONTROL DE APROBACIÓN

ESTADO	FECHA	NOMBRE	CARGO
ELABORÓ	2025-06-17	MARYURY FORERO BOHORQUEZ	ENLACE MIPG
REVISÓ	2025-06-19	SANDRA ESPERANZA AVILA PEREZ	REFERENTE MIPG
APROBÓ	2025-06-19	DANIEL SANCHEZ ROJAS	LIDER DE PROCESO
AVALÓ	2025-06-20	DANIEL SANCHEZ ROJAS	JEFE DE LA OFICINA ASESORA DE PLANEACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN

COLABORADORES

NOMBRE
JONATHAN GONZALEZ BOLANOS
MARYURY FORERO BOHORQUEZ