POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

HISTORICO DE CAMBIOS		
Versión	**Fecha**	**Cambios Realizados**
01	Enero 2014	Emisión inicial
02	Septiembre 2015	Se ajustan los manejos de las contraseñas y actualización del servicio de correo bajo la plataforma Google
03	Enero 2017	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.
04	Septiembre 2021	Actualización de todos los capítulos de la política de acuerdo con la nueva normatividad establecida

Elaboró:	**Revisó:**	**Aprobó:**	**Avaló:**
Andrés Briceño Díaz Oficial de Seguridad de la Información y Ciberseguridad	**Edgar Alfonso Cipagauta Pedraza** Profesional Universitario Oficina Asesora de Planeación y Tecnologías de la Información **Camila Crespo Murillo** Contratista Oficina Asesora de Planeación y Tecnologías de la Información	**Carlos Alfonso Gaitán Sánchez** Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información	**Carlos Alfonso Gaitán Sánchez** Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La seguridad de la información dispone de lineamientos técnicos y legales para preservar la confidencialidad, integridad y disponibilidad de la información del Instituto Distrital de las Artes – Idartes, incluye la adopción de controles que respondan a las necesidades de la entidad y que contribuyan al alcance de las metas institucionales.

La Dirección General del Instituto Distrital de las Artes – Idartes, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad. Para el Instituto Distrital de las Artes – Idartes, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

Esta política debe ser aplicada por todos los (as) funcionarios (as), contratistas, proveedores, consultores y todo personal externo que utilice los servicios informáticos que ofrece la Entidad, deben conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional. Esta política se actualizará por parte de la Oficina Asesora de Planeación y Tecnologías de la Información, de acuerdo con las disposiciones legales, técnicas o institucionales que defina el Estado colombiano, el Distrito Capital y/o el Instituto Distrital de las Artes – Idartes.

El Idartes es un Establecimiento público del orden distrital, con personería jurídica, autonomía administrativa, financiera y patrimonio propio, encargado de garantizar el ejercicio de los derechos culturales, mediante la promoción de las artes en el Distrito Capital, contribuyendo al desarrollo de sujetos creativos, sensibles, respetuosos de la diferencia, aportando a la construcción de una ciudad incluyente y solidaria, la mayoría de la información generada en las diferentes Subdirecciones requiere de controles efectivos, de procedimientos internos para que permita brindar las condiciones para custodiar sus datos, sistemas de información, plan de tratamientos de riesgos de seguridad y privacidad de la información y acción para el uso y salvaguarda de la información, por lo anterior es pertinente y necesario planear e implementar una Política de Seguridad de la Información en Idartes de manera gradual y transversal, en sus procesos, tomando como base el proceso de gestión de tecnologías de la información y las comunicaciones TIC, por ser este el que tiene en su hacer, la seguridad de la información del Instituto.

El habilitador de seguridad de la Política Nacional de Gobierno Digital y Seguridad de la Información prepara para la transformación digital y para brindar servicios ciudadanos digitales seguros por medio del fortalecimiento de la seguridad de la información en la Entidades del estado al aplicar un enfoque de gestión de seguridad y privacidad a los activos de información. La presente política busca el fortalecimiento de la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en el Idartes está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos. Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado y la implementación de políticas de seguridad digital se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de seguridad y privacidad de la información como base de la aplicación del concepto de Seguridad Digital.

2. OBJETIVOS

El Instituto Distrital de las Artes – Idartes, en su propósito de dar cumplimiento con la política establecida de seguridad y privacidad de la información establece los siguientes objetivos:

- Establecer las políticas de seguridad de la información necesarias para la protección de los activos de información, las cuales se desarrollan alineadas con el 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 *Modelo de Seguridad y Privacidad de la Información* - MSPI como mecanismo para brindar a los ciudadanos y colaboradores confianza digital en torno al uso 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 organización, 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
- Cumplir con los principios de seguridad de la información de confidencialidad, integridad y disponibilidad.
- Cumplir con los controles de seguridad para el cumplimiento normativo y regulatorio de la Entidad.
- Sensibilizar los controles de seguridad y privacidad de la información en los colaboradores, funcionarios, contratistas, terceros y demás partes interesadas.
- Gestionar la debida clasificación acorde a la función pública.
- Buscar la protección de los activos de información del Idartes.

3. ALCANCE Y 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 y disponibilidad 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, 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.

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 y privacidad de la información se refiere.

4. MARCO LEGAL Y/O NORMATIVO

El instituto distrital de las artes Idartes acoge las normas vigentes de seguridad de información, protección de datos personales y directrices de ciberseguridad a nivel nacional y territorial aplicando las prácticas y estándares recomendados para su cumplimiento.

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
Ley	23	1982	Sobre Derechos de Autor. Congreso de la República. Disponible en Línea http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431	X		
CONSTITUCIÓN POLÍTICA DE COLOMBIA	1991	1991	Artículo 15. “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Disponible en Línea: http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15	X		
Ley	527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276.	X		

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
Ley	1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488	X		
Resolución	305	2008	Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre. Expedida por: la Comisión Distrital de Sistemas (CDS) de Bogotá.		X	
Ley	1273	2009	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492	X		
Decreto	235, Art.1-4	2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones pública	X		

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
Ley	1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43292.	X		
Decreto	4632	2011	Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones. Disponible en Línea: http://wsp.presidencia.gov.co/Normativa/Decretos/2011/Documents/Diciembre/09/dec463209122011.pdf	X		
Directiva	22	2011	Estandarización de la información de identificación, caracterización, ubicación y contacto de los ciudadanos y ciudadanas que capturan las entidades del Distrito Capital. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45545. Expedida por el Alcalde Mayor de Bogotá.		X	
Decreto	2609	2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado". Disponible en Línea: http://www.mintic.gov.co/portal/604/articles3528_documento.pdf.	X		

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
Ley Estatutaria	1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.	X		
Decreto	1377	2013	Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5364.	X		
Ley	1621	2013	Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y también se dictan otras disposiciones.	X		
Ley	1712	2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882.	X		
Decreto	886	2014	Reglamentar la información mínima que debe contener el Registro Nacional de Bases de Datos, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los Responsables del Tratamiento. Disponible en línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=57338.	X		

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
Decreto	103	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556.	X		
Decreto	1494	2015	Por el cual se corrigen yerros en la Ley 1712 de 2014. Disponible en Línea: http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201494%20DEL%2013%20DE%20JULIO%20DE%202015.pdf.	X		
Decreto	1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones". (Artículo 1.1.2.3 derogado por el Artículo 1 del Decreto 045 de 15 de enero de 2021)	X		
Decreto	415	2016	Por el cual se adiciona el Decreto único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de información y las comunicaciones.	X		
Decreto	1499	2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.	X		
Decreto	1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del	X		

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
			sector de Tecnologías de la Información y las Comunicaciones. Disponible en Línea: https://www.mintic.gov.co/portal/604/articles-74903_documento.pdf. Expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones			
Resolución	160	2019	Por la cual se deroga la resolución 673 de 2013 y se adopta el manual de política de seguridad de la información del sitio web en materia de datos personales y protección de datos personales recaudados en las bases de datos creadas en la entidad			X
Directiva	02	2019	Simplificación de interacción digital los ciudadanos y el estado. Expedida por Presidente de la Republica.	X		
Conpes	3975	2019	POLÍTICA NACIONAL PARA LA TRANSFORMACIÓN DIGITAL E INTELIGENCIA ARTIFICIAL. Establece dentro de sus acciones la formulación de una política pública sobre ciberseguridad		X	
Ley	1955	2019	Presidencia de Colombia. Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)	X		
Decreto	2106	2019	Departamento Administrativo De La Función Pública. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración		X	

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
			pública Cap. II Transformación Digital Para Una Gestión Pública Efectiva			
Circular	001	2019	Normativa de la Superintendencia de Industria y Comercio de Colombia, sobre la obligación de registro de bases de datos.		X	
Ley	1978	2019	Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones. (Declarada exequible por la Sentencia C-127 de 2020 de la Corte Constitucional).	X		
Decreto	620	2020	Departamento Administrativo De La Función Pública. Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales		X	
Conpes	3995	2020	POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL. Establece medidas para desarrollar la confianza digital a través de la mejora la seguridad digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías		X	
Decreto	045	2021	“Por el cual se derogan el Decreto 704 de 2018 y el artículo 1.1.2.3. del Decreto 1078 de 2015, Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”		X	
Directiva	003	2021	Lineamientos para el uso de servicios en la nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.	X		

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
Presidencial						
Resolución	00500	2021	Ministerio De Tecnologías De La Información y las Comunicaciones. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital		X	

4.1. Documentos de referencia

Tipo de documento	Título del documento	Código	Origen	
			Externo	Interno
Decreto Distrital	Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión Nacional y se dictan otras disposiciones	591 de 2018	X	
Norma Técnica Internacional ISO 27001, 27002, 27005	Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información en una organización pública o privada	ISO/IEC 27001, 27002, 27005	X	
Norma Técnica Internacional ISO 31000: 2018	Es el estándar para la gestión de riesgos y describe cuatro pasos básicos – Identificación de riesgos, análisis de riesgos, valoración de riesgos y tratamiento de riesgos– para llevar a cabo un proceso de evaluación de riesgos exitoso; esto con el fin de identificar aquellas amenazas que pueden ser un obstáculo para que la organización logre sus metas.	ISO/IEC 31000	X	
MANUAL DE GOBIERNO DIGITAL	Para la Implementación de la Política de Gobierno Digital, entidades del orden nacional; Modelo de Seguridad y Privacidad de la Información-MSPI; Formato Política SGSI – MSPI para la Política de Gobierno Digital.	Versión 7	X	

Tipo de documento	Título del documento	Código	Origen	
			Externo	Interno
Documento Maestro del Modelo de Seguridad y Privacidad de la Información Marzo 2021	Actualización del documento para la implementación del modelo MSPI en la entidades del estado	Versión 4	X	

5. DEFINICIONES

Activos de información: Corresponde a elementos tales como bases de datos, documentación, manuales de usuarios, planes de continuidad, etc.

Activos de software: Son elementos tales como: Aplicaciones de software, herramientas de desarrollo, y utilidades adicionales.

Activos físicos: Se consideran activos físicos elementos tales como: Computadores, portátiles, módems, impresoras, máquinas de fax, equipos de comunicaciones, PBX, cintas, discos, UPS, muebles etc.

Afinamiento de bases de datos: Son las actividades relacionadas con mantener el desempeño y la eficiencia de la base de datos. Estas actividades se realizan cuando las necesidades del negocio requieren mayor rendimiento en sus transacciones y/o almacenamiento.

Back-up (copia de respaldo): Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos o CDs), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto.

Back-ups incrementales: Una operación de back up incremental sólo copia los datos que han variado desde la última operación de back up de cualquier tipo. Se suele utilizar la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último back up.

Clave: Contraseña o password, es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La clave debe mantenerse en secreto ante aquellos a quien no se le permite el acceso.

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

Cuarto de Comunicaciones: Es un área utilizada para el uso exclusivo de equipos asociados con el sistema de cableado de telecomunicaciones de la Entidad. El cuarto de telecomunicaciones o datacenter, debe ser capaz de albergar los equipos de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado.

Cuenta de Usuario: Credencial que identifica a un usuario para autenticarse sobre una plataforma tecnológica.

Custodio de la información: es el encargado de la administración de seguridad de información. Dentro de sus responsabilidades se encuentra la gestión del Plan de Seguridad de Información, así como la coordinación de esfuerzos entre el personal de sistemas y los responsables de las otras áreas de la Entidad, siendo estos últimos los responsables de la información que utilizan. Asimismo, es el responsable de promover la seguridad de información en toda la Entidad con el fin de incluirla en el planteamiento y ejecución de los objetivos institucionales.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información de la Entidad, después del resultado de los procesos de evaluación y tratamiento de riesgos.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Desactivación de cuenta de usuario: Es un estado de la cuenta de usuario que se asigna cuando el propietario de la cuenta termina definitivamente su vínculo con la Entidad.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Firewall: Un cortafuego (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Freeware: Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.

Hacking ético: Es una forma de referirse al acto de una persona, conocido como hacker, que utiliza sus conocimientos de informática y seguridad para encontrar vulnerabilidades o fallas de seguridad en el sistema, con el objetivo de reportarlas en la organización para que se tomen todas las medidas necesarias que posibilite prevenir una catástrofe cibernética, como el robo de información.

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento los cuales deben ser exactos.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

Inventario Tecnológico: Se refiere al inventario de dispositivos electrónicos que hacen parte de los activos de la Entidad.

Licencias de tipo GNU (General Public License): Es la licencia más usada en el mundo del software y garantiza a los usuarios finales (personas, organizaciones, compañías) la libertad de usar, estudiar, compartir y modificar el software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

Log de transacciones: Es un archivo, donde se registran todas las transacciones de las bases de datos.

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse.

Mecanismos de bloqueo: Son los mecanismos necesarios para impedir que los usuarios, tanto de los sistemas de información como de los servicios, tengan acceso a estos sin previa autorización, ya sea por razones de seguridad, falta de permisos, intentos malintencionados o solicitud de los propietarios de la información.

Niveles de respaldo de información: Hace referencia a los diferentes ambientes en los cuales las copias de seguridad se guardan de manera oportuna con el fin de tener varios niveles de

recuperación de la información en caso de desastre. Actualmente la Entidad cuenta con niveles de respaldo, las unidades de almacenamiento extraíble, cintas y/o replicación de las bases de datos en el datacenter.

OTP (One Time Password): Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.

Phishing (cosecha y pesca de contraseñas): Es un delito cibernético con el que por medio del envío de correos se engaña a las personas invitándolas a que visiten páginas web falsas de entidades bancarias o comerciales. Allí se solicita que verifique o actualice sus datos con el fin de robarle sus nombres de usuarios, claves personales y demás información confidencial.

Plan de Contingencia: Procedimientos alternativos de una Entidad cuyo fin es permitir el normal funcionamiento de esta y/o garantizar la continuidad de las operaciones, aun cuando alguna de sus funciones se vea afectadas por un accidente interno o externo.

Plataforma Tecnológica: Una plataforma tecnológica es una agrupación de equipamientos técnicos y humanos destinados a ofrecer unos recursos tecnológicos de elevado nivel acompañados de excelentes conocimientos científicos a una comunidad de usuarios, públicos y privados, tanto a nivel local, regional como nacional.

Propiedad intelectual: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Rack: Soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de distintos fabricantes. También son llamados bastidores, cabinas, gabinetes o armarios.

RSS (Really Simple Syndication): RSS son las siglas de Really Simple Syndication, un formato XML para sindicar o compartir contenido en la web. Se utiliza para difundir información actualizada frecuentemente a usuarios que se han suscrito a la fuente de contenidos. El formato permite distribuir contenidos sin necesidad de un navegador, utilizando un software diseñado para leer estos contenidos RSS tales como Internet Explorer, entre otros.

Seguridad de la información: Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los

activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información.

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.

Servicios TIC: El concepto de Servicio TIC consiste en dar soporte, de forma integrada y personalizada, a todas estas herramientas que necesita hoy en día el profesional de empresa para realizar su trabajo. Los elementos del Servicio TIC son:

- Los dispositivos: PC, portátiles, agendas electrónicas, impresoras, teléfonos, sistemas de videoconferencia, etc.
- La Red de Área Local corporativa (LAN). Así como las comunicaciones de voz incluyendo el teléfono y ahora llega el momento de proporcionar y gestionar los PC y la electrónica de red necesarios para las comunicaciones de datos.
- Las comunicaciones de voz y datos WAN (Red de Área Remota), que incluyen tanto las redes privadas corporativas como el acceso a redes públicas como Internet. La integración de las comunicaciones WAN y estas cada vez se requieren con las comunicaciones LAN.
- Los servicios y aplicaciones desde la red.

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 de tiempo, o con unas funciones básicas permitidas. para adquirir el software de manera completa es necesario un pago económico.

Sistemas de Información: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Sistema Operativo (S.O): Es el software básico de un computador que provee una interface entre el resto de los programas, los dispositivos de hardware y el usuario.

Sniffer: Es una aplicación especial para redes informáticas, que permite como tal capturar los paquetes que viajan por una red.

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:

a) Documentos de Archivo (físicos y electrónicos).
b) Archivos institucionales (físicos y electrónicos).
c) Sistemas de Información Corporativos.
d) Sistemas de Trabajo Colaborativo.
e) Sistemas de Administración de Documentos.
f) Sistemas de Mensajería Electrónica.
g) Portales, Intranet y Extranet.
h) Sistemas de Bases de Datos.
i) Discos duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc.
j) Cintas y medios de soporte (back up o contingencia).
k) Uso de tecnologías en la nube.

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".

Vulnerabilidad: debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

Webcam - Cámara Web: Una cámara web o cámara de red (en inglés: webcam) es una pequeña cámara digital conectada a una computadora la cual puede capturar imágenes y transmitirlas a través de Internet, ya sea a una página web o a otra u otras computadoras de forma privada.

6. RESPONSABILIDADES

6.1. Compromiso de la Dirección General

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

- 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 de seguridad de la información.
- Debe comunicar a la organización 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 de la Entidad.

6.2. Compromiso Comité Institucional de Gestión y Desempeño del IDARTES

- Actualizar y presentar la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- Analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- Verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.
- 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.

6.3. Compromiso Area de Control Interno

Las auditorías y seguimientos a la gestión de tecnologías de la información se realizarán conforme a los lineamientos definidos por la Area de Control Interno con el acompañamiento de la Oficina de Planeación y Tecnologías de la Información.

6.4. 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 de Seguridad de la Información, asegurando así los recursos adecuados y promoviendo así una cultura activa de seguridad en la Entidad.
- Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de información y todos sus capítulos, el uso de los servicios tecnológicos en toda la entidad de acuerdo a las mejores prácticas y lineamientos de la Dirección General del Instituto Distrital de las Artes – Idartes y directrices del Gobierno Nacional.
- 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, con el fin de evitar modificación no autorizada o intencional o el uso indebido de los activos de la organización.
- 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 estén en contra de la seguridad de la información y de la infraestructura tecnológica de la entidad a las partes afectadas del Instituto Distrital de las Artes – Idartes.
- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la Entidad.
- Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.
- Administrar las reglas 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 asegurar los datos e información gestionados en la Entidad.
- Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por las propiedades de integridad, accesibilidad y disponibilidad, características de la información al interior de la entidad. Esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son parte integral del apoyo de la solicitud.

- Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Dirección General y las diferentes direcciones.
- Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.

6.5. Compromiso del grupo de tecnología

- 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 a 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 toda la entidad de acuerdo a las mejores prácticas y directrices de la Entidad 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 mesa de ayuda actualmente implementados en la entidad.

6.6. Responsabilidades de los propietarios de la información

Son propietarios de la información cada uno de los líderes de las oficinas 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 a 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 a 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.

6.7. 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 que esté bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
- Proteger la información a la cual acceden y procesen, 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 no autorizada.
- Reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos designados para el desarrollo de sus funciones.
- Usar 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 de Seguridad de la Información.*
- Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección General y Control Interno de la entidad puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad de la entidad, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la entidad. Esta

revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.

- 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.

6.8. Gestión de la Política de Seguridad de la Información

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

6.8.1. Documento de la Política de Seguridad de la Información.

La Dirección General debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes

6.8.2. Revisión de la Política de Seguridad de la Información.

El documento de la *Política de Seguridad de la Información* se debe revisar mínimo una vez al año o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz

6.9. Organización interna

Se debe gestionar la seguridad de la información dentro de la organización.

6.9.1. Compromiso de la dirección con la seguridad de la información.

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

6.9.2. Coordinación de la seguridad de la información.

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

6.9.3. 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 organización para la protección de la información.

6.10. Partes externas

Se busca mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.

6.10.1 Identificación de los riesgos relacionados con las partes externas.
Se identificarán los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.

6.10.2. Consideraciones de la seguridad en los acuerdos con terceras partes
Los acuerdos con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los requisitos pertinentes de seguridad

7 GESTIÓN DE ACTIVOS

7.1 Responsabilidad por los activos
Mantener la protección adecuada de los activos organizacionales.

7.1.1. Inventario de activos
Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.

- El Instituto Distrital de las Artes – Idartes es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores del Instituto Distrital de las Artes – Idartes (denominados "usuarios") que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).
- Atender los lineamientos de un equipo interdisciplinario conformado por la Oficina Asesora de Planeación y Tecnologías de la Información, Gestión Documental y la Oficina Asesora Jurídica serán responsables de realizar el inventario de los activos de información para su control y administración, de acuerdo al formato que esta Oficina determine para tal fin, estos recursos deben estar compuestos por medios físicos (archivo documental), digitales (bases de datos digitales y manuales, sistemas de información, aplicaciones de software, sistemas de back up) electrónicos (servidores, computadores personales y de comunicaciones (redes LAN y Wifi, firewall, sistemas de control de comunicaciones), recurso humano con roles y responsabilidades para acceso a la información sobre los cuales se aplicarán regulaciones internas para el uso controlado y seguro de la misma.

7.1.2 Propiedad de los activos
Toda la información y los activos asociados con los servicios de procesamiento de información deben ser propiedad de una parte designada de la organización.

- El Instituto Distrital de las Artes – Idartes es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios del Instituto Distrital de las Artes – Idartes y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

7.1.3 Uso aceptable de los activos

Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.

- El Instituto Distrital de las Artes – Idartes implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.
- Todos los servidores, contratistas y terceras partes, que usen activos de información de propiedad del Instituto Distrital de las Artes – Idartes son responsables de cumplir y acoger con integridad la Política de Seguridad para dar un uso racional y eficiente a los recursos asignados.

7.2 Clasificación de la información

7.2.1 Directrices de clasificación

La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización. Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sean de carácter institucional.

- El Instituto Distrital de las Artes - Idartes, consciente de la necesidad de asegurar que la información reciba el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley y el Instituto Distrital de las Artes - Idartes, define reglas de cómo clasificar la información, liderado por el proceso de *Gestión Documental* de la Entidad.
- Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel visual u otro que genere el Instituto Distrital de las Artes - Idartes como:
    - Formularios/ comprobantes propios o de terceros.
    - Información en los sistemas, equipos informáticos, medios magnéticos y/o electrónicos o medios físicos en papel.
    - Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
    - Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.
- Los usuarios responsables de la información del Instituto Distrital de las Artes - Idartes, deben identificar los riesgos a los que está expuesta la información de sus áreas,

teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

7.2.2 Etiquetado y manejo de información

Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.

Gestionar el activo de información como un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como "Valiosa" para el Instituto Distrital de las Artes - Idartes; Independiente del tipo de activo, se deben considerar las siguientes características:

- El activo de información es reconocido como valioso para el Instituto Distrital de las Artes – Idartes.
- No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
- Forma parte de la identidad de la organización y sin el cual el Instituto Distrital de las Artes - Idartes puede estar en algún nivel de riesgo. (La determinación del nivel y tipo de riesgo se estima sobre la base del Modelo de seguridad y privacidad de la información - MPSI del Instituto Distrital de las Artes - Idartes).
- Los niveles de clasificación de la información valiosa que se ha establecido son:
    - Información pública reservada,
    - Información pública clasificada (privada y semi-privada),
    - Información pública.

8 SEGURIDAD DE LOS RECURSOS HUMANOS

8.1 Antes de la contratación

Asegurar que los empleados, contratistas por prestación de servicios y usuarios de terceras partes entienden sus responsabilidades y uso adecuado de la seguridad de información en los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de la infraestructura tecnológica.

- La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad, disponibilidad y accesibilidad por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.
- Informar al personal desde su ingreso y en forma continua, cualquiera sea su situación laboral con la entidad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.
- Definir las sanciones que se aplicarán en caso de incumplimiento.

8.1.1. Roles y responsabilidades

Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes para la seguridad, de acuerdo con la Política de Seguridad de la Información de la Entidad.

- Todo empleado llámese funcionario, contratista o terceros nuevo del Instituto Distrital de las Artes - Idartes deberá de contar con la inducción sobre la *Política de Seguridad de la Información*, a través de la Oficina Asesora de Planeación y Tecnologías de la Información apoyado en el Area de Talento Humano y la Oficina de Contratación, donde se den a conocer los roles y responsabilidades para los usuarios y las sanciones que pueden existir en caso de incumplimiento.
- Cuando un individuo es contratado para un rol de seguridad de la información específico, Idartes debe asegurar que el candidato tenga la competencia necesaria para desempeñar el rol de seguridad; validando idoneidad para desempeñar el rol, especialmente si es crítico para la organización.
- Cuando un trabajo, ya sea una asignación o una promoción, implique que la persona tenga acceso a las instalaciones de procesamiento de información, y en particular, si ahí se maneja información confidencial, se debe realizar verificaciones que garanticen la seguridad de la información.

8.1.2 Selección

Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

- El Instituto Distrital de las Artes - Idartes realizará los controles previos de verificación del personal en el momento en que se solicita el cargo/contratista. Estos controles incluyen antecedentes disciplinarios, procuraduría, personería y judiciales y todos los aspectos que a tal efecto requiera la entidad.

8.1.3 Términos y condiciones laborales.

Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.

- Todos los usuarios de bienes y servicios informáticos del Instituto Distrital de las Artes - Idartes deben firmar la aceptación del Acuerdo de confidencialidad y uso adecuado de los recursos informáticos y de información del Instituto Distrital de las Artes - Idartes.

8.2 Durante la vigencia de la contratación

Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

8.2.1 Responsabilidades de la dirección

La Dirección debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización.

Todos los servidores públicos del Instituto Distrital de las Artes - Idartes y cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la entidad recibirán una adecuada capacitación y actualización periódica en materia de normas y procedimientos del Instituto Distrital de las Artes - Idartes. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

- La Oficina Asesora de Planeación y tecnologías de información se apoyará en el Área de Talento Humano para programar capacitaciones entorno a la política.
- Cada tiempo determinado se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo con el estado de ese momento.
- Al personal que ingrese al Instituto Distrital de las Artes - Idartes se le indicará el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales. Se habilitarán los medios técnicos necesarios para comunicar y socializar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

8.2.3 Proceso disciplinario

La Oficina Asesora de Planeación y Tecnologías de la Información publicará en la Intranet el documento *Política de Seguridad de la Información*, socializa su contenido y hará cumplir su alcance. El desconocimiento de la política de seguridad de la información del Instituto Distrital de las Artes - Idartes, por parte de funcionarios, contratistas y terceros puede generar acciones disciplinarias. Las investigaciones disciplinarias y las respectivas sanciones les corresponden a las instancias autorizadas por el Idartes.

Actuaciones que conllevan a la violación de la seguridad de la información establecidas por el Instituto Distrital de las Artes - Idartes:

- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No realizar la debida custodia de la información y de los activos de información a su cargo.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico u ofensivo, cadenas de correos para fines no institucionales y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Negligencia en el cuidado y custodia de los equipos, dispositivos portátiles o móviles entregados para actividades propias del Instituto Distrital de las Artes - Idartes.
- No cumplir con las actividades designadas para la protección de los activos de información del Instituto Distrital de las Artes - Idartes.
- Realizar cambios no autorizados en la plataforma tecnológica del Instituto Distrital de las Artes - Idartes.
- Acceder, almacenar o distribuir pornografía.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el Oficina Asesora de Planeación y Tecnologías de la Información del Instituto Distrital de las Artes - Idartes.

8.3 Terminación o cambio en la contratación

Asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su vínculo laboral de forma ordenada.

8.3.1 Responsabilidades en la terminación contractual

Se deben definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio del vínculo laboral.

Todos los servidores públicos al finalizar su relación contractual con el Instituto Distrital de las Artes - Idartes, deberán tramitar el formato de paz y salvo correspondiente mediante el diligenciamiento del documento definido por la Entidad para tal fin. Se deben realizar las siguientes actividades de control:

- El supervisor contractual y/o jefe y/o director y/o subdirector, deberá recibir copia de la información generada por el servidor público en la cual debe incluir los usuarios y contraseñas para archivos que haya generado y estén protegidos para su apertura.

- La oficina de contratación incluirá las obligaciones relativas a la seguridad de la información en las descripciones de las actividades de los contratistas, informará a todo el personal que ingresa, sus obligaciones respecto al cumplimiento de la *Política de Seguridad de la Información*, gestionará los Compromisos de Confidencialidad con el contratista para validar su cumplimiento al finalizar la gestión contractual.

8.3.2 Devolución de activos informáticos

Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación. Los funcionarios, contratistas y terceros que tengan activos asignados por la entidad deben realizar la entrega de los mismos con el fin de adelantar los paz y salvos correspondientes a la ejecución contractual.

8.3.3 Retiro de los derechos de acceso

Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio.

- Los administradores de los diferentes sistemas de información deberán desactivar las cuentas de usuario.
- El administrador del dominio deberá verificar el vencimiento de la cuenta e inactivar las credenciales, con el fin de asegurar, que el usuario no pueda iniciar una sesión con las credenciales que en su momento le fueron otorgadas.
- El administrador de la plataforma del correo electrónico designado por el Instituto Distrital de las Artes - Idartes, procederá a generar una copia del contenido del buzón del correo y de la información que tenga almacenada en la unidad de drive sobre el correo. Una vez tenga almacenada la copia del buzón, procederá a eliminar la cuenta.

9. SEGURIDAD FÍSICA Y DEL ENTORNO

9.1 Áreas seguras

Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.

9.1.1 Perímetro de seguridad física

Se deben utilizar perímetros de seguridad como paredes, puertas de acceso controladas para proteger las áreas que contienen información y servicios de procesamiento de información.

- El centro de cómputo, los cuartos de distribución del cableado lógico y eléctrico y el cuarto de ubicación de las UPS en el sótano deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá estar acompañada permanentemente por el personal profesional y/o técnico de la Oficina Asesora de Planeación y Tecnologías de la Información

- La entrada o salida a cada uno de los recintos mencionados deben quedar registrados en un documento bitácora para el control y seguimiento, el acceso a esos sitios, deben contar con una puerta, la cual debe permanecer cerrada con llave, las llaves de acceso las cuales serán custodiadas con el apoyo del guarda correspondiente para desarrollo de actividades propias de las funciones de la Oficina Asesora de Planeación y Tecnologías de la Información.

9.1.2 Controles de acceso físico.

Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.

- Aplicar gestión de ingresos con un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación.
- El porte del carné físico de identificación en un lugar visible es de uso obligatorio dentro de las instalaciones de la Entidad, en caso de que el carné sea digital debe estar disponible para la verificación en todo momento.
- Está prohibido prestar el carné de identificación, se considera como suplantación de identidad por parte de la persona que lo usa sin ser la persona autorizada.
- La pérdida del carné de identificación debe ser reportado al Area de Talento Humano por medio de correo electrónico.

9.1.3 Seguridad de oficinas, recintos e instalaciones.

Se debe aplicar la seguridad física para oficinas, recintos e instalaciones.

- El ingreso de computadores que no sean de propiedad del instituto distrital de las artes – Idartes deben ser registrados en un libro de registro de equipos, o el que se destine para tal fin en la empresa de vigilancia indicando la fecha, hora de entrada, hora de salida, nombre y apellido, marca, serial y firma; de igual manera a la hora de salida se debe verificar que el equipo que está saliendo sea el mismo número de serie del que entró con la persona responsable.
- Tener un registro de la fecha y hora de entrada y salida de los visitantes, y todos los visitantes deben ser supervisados a menos que su acceso haya sido aprobado previamente; solo se les debe otorgar acceso para propósitos específicos autorizados y se deben emitir instrucciones sobre los requisitos de seguridad del área y de los propósitos de emergencia.
- Las identidades de los visitantes se deben autenticar por los medios apropiados;
- Establecer que el acceso a las áreas en las que se procesa o almacena información confidencial debe ser restringido a los individuos autorizados solamente mediante la implementación de controles de acceso apropiados,
- Definir directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial no deben ser accesibles a ninguna persona no autorizada

9.1.4 Protección contra amenazas externas y ambientales.
Se deben diseñar y aplicar protecciones físicas contra daño por desastre natural o artificial.

- En las sedes Instituto Distrital de las Artes - Idartes se debe contar con sistema contra incendio debe estar en un perímetro de seguridad, tener alarmas, y así mismo, estar probadas, para establecer el nivel requerido de resistencia de acuerdo con normas y deben funcionar de manera segura de acuerdo a los lineamientos en materia de protección de incendios

9.1.5 Trabajo en áreas seguras.
Aplicar la protección física y las directrices para trabajar en áreas seguras.

- El ingreso a áreas denominadas como seguras será exclusiva del referente de dicha área o unidad de gestión.
- El responsable del área segura o a quien éste designe debe supervisar los trabajos realizados por terceros en el área segura a su cargo.
- El área Administrativa garantizará el funcionamiento de cada uno de los controles de seguridad establecidos para cada una de sus áreas a cargo, como, por ejemplo, controles de acceso, puertas cerradas, extintores entre otros.
- Se deben usar los elementos de protección personal que el área segura requiera.
- Está prohibido fumar y el consumo de bebidas alcohólicas en donde exista algún activo de información de la plataforma tecnológica del instituto distrital de las artes – Idartes.

9.1.6 Áreas de carga, despacho y acceso público
Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deben controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.

- En las sedes que tengan zona de descarga, el acceso a las zonas de despacho y carga debe ser autorizado por la Administración del edificio.
- En las sedes que tengan parqueadero o zonas de descarga, todo vehículo que ingrese a dejar o retirar elementos de la Entidad debe estar previamente autorizada por la Administración.

9.2 Seguridad de los equipos
Evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.

9.2.1 Ubicación y protección de los equipos.
Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado

- Los equipos de cómputo (Computadores, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa de la Oficina Asesora de Planeación y Tecnologías de la Información y el correspondiente acompañamiento técnico.
- Los particulares en general, entre ellos, los familiares de los funcionarios públicos, no deberían estar autorizados para utilizar los recursos informáticos de la Entidad.

9.2.2 Servicios de suministro

Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro. Los equipos tecnológicos del instituto distrital de las artes – Idartes están protegidos contra posibles fallas en el suministro de energía u otras anomalías eléctricas. Para asegurar la continuidad del suministro de energía:

- Múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- Suministro de energía interrumpida mediante UPS para asegurar el apagado regulado y sistemático.
- Equipos de UPS inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
- Interruptores de emergencia ubicados en sitios estratégicos a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica.
- Cumplir con las especificaciones en materia de suministro de los fabricantes de equipos
- Evaluar regularmente en cuanto a su capacidad para estar al ritmo del crecimiento e interacciones del negocio con otros servicios de soporte

9.2.3 Seguridad del cableado.

El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deben estar protegidos contra interceptaciones o daños.

- Uso de conductos independientes para separar el cableado eléctrico del cableado de comunicaciones, evitando interferencias.
- Acceso controlado a los módulos y cuartos de cableado.
- Protección del tendido del cableado troncal (vertical) mediante la utilización de ductos blindados.
- Establecer que las líneas de potencia y de telecomunicaciones que entran a instalaciones de procesamiento de información, estas deben ser subterráneas en donde sea posible, o deben contar con una protección alternativa adecuada

9.2.4 Mantenimiento de los equipos.

Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad. Se realizará el mantenimiento periódico de los equipos informáticos para asegurar su disponibilidad e integridad permanentes. Para ello se debe tiene en cuenta:

- Únicamente el personal calificado y autorizado puede realizar actividades de mantenimiento y llevar a cabo reparaciones o modificaciones en los equipos tecnológicos.
- Se registrarán todos los mantenimientos preventivos y las acciones correctivas que se realicen en los equipos tecnológicos.
- Establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos activos y servidores.
- Establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar por el grupo de tecnología para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.

9.2.5 Seguridad de los equipos fuera de las instalaciones.

Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización. Los activos no serán retirados de las instalaciones del instituto distrital de las artes – Idartes y/o sus sedes anexas, sin una autorización formal de la Oficina Asesora de Planeación y Tecnologías de la Información y el area de Administrativa.

- Identificar a los empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio y el acompañamiento del personal de la Oficina Asesora de Planeación y Tecnologías de la Información
- Definir cuando sea necesario y apropiado, registrar los activos se retiran del sitio y cuando se hace su devolución;
- Documentar la identidad, el rol y la vinculación de cualquiera que maneje o use activos, y devolver esta documentación con el equipo, la información y el software.

9.2.6 Seguridad en la reutilización o eliminación de los equipos.

Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.

- Se eliminará toda la información que contenga cualquier equipo informático que se requiera retirar, realizando previamente las respectivas copias de resguardo.
- Mantener los equipos de acuerdo con la vida útil y especificaciones de servicio recomendados por el proveedor;

9.2.7 Retiro de activos

Ningún equipo, información ni software se deben retirar sin autorización previa.

- Identificar a los empleados, contratistas y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio y el acompañamiento del personal de la Oficina Asesora de Planeación y Tecnologías de la Información;

- Definir cuando sea necesario y apropiado, registrar los activos se retiran del sitio y cuando se hace su devolución;
- Documentar la identidad, el rol y la vinculación de cualquiera que maneje o use activos, y devolver esta documentación con el equipo, la información y el software.

10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.1 Procedimientos operacionales y responsabilidades

Asegurar la operación correcta y segura de los servicios de procesamiento de información.

10.1.1 Documentación de los procedimientos de operación

Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.

- Se documentará y mantendrá actualizados los procedimientos de la gestión de tecnologías de la información necesarios para implementar esta Política. Dichos procedimientos y sus actualizaciones serán revisados al menos anualmente por el responsable del proceso.

10.1.2 Gestión del cambio.

Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información, el responsable del desarrollo e implementación de los Sistemas de Información controlará y dará seguimiento a que los cambios en los ambientes productivos no afecten la seguridad de estos ni de la información que soportan.

10.1.3 Distribución de funciones.

Las funciones y las áreas de responsabilidad en operaciones sobre la plataforma tecnológica se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización

- La Oficina Asesora de Planeación y Tecnologías de la Información, realizara controles como:
  - Monitoreo de las actividades.
  - Registros de control y seguimiento.
- Se debe asegurar la independencia de las funciones de auditoría de seguridad, tomando precauciones para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización.

10.1.4 Separación de las instalaciones de desarrollo, ensayo y operación.

Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

- Definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de operaciones.
- Establecer que el software de desarrollo y de operaciones debe funcionar en diferentes sistemas o procesadores de computador y en diferentes dominios o directorios;
- Definir que los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales;
- Definir que solo en circunstancias excepcionales, las pruebas no se deben llevar a cabo en los sistemas operacionales;
- Establecer que los usuarios deben usar diferentes perfiles de usuario para sistemas operacionales y de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error;
- Prohibir a los usuarios compartir contraseñas en estos sistemas.
- Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
- Cumplir con los lineamientos de la Política de Desarrollo de Software establecida por el Idartes

10.2 Gestión de la prestación del servicio por terceras partes
Implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes, para lo cual se cumplirán los siguientes controles.

10.2.1 Prestación del servicio
En los contratos que se manejen con proveedores de tecnología se deben garantizar controles de seguridad, las definiciones del servicio y los niveles de prestación de los servicios TI

10.2.2 Monitoreo y revisión de los servicios por terceras partes
Los servicios, reportes y registros suministrados por terceras partes en la ejecución contractual se deben controlar y realizar el seguimiento para garantizar el óptimo funcionamiento de los servicios TI.

10.3 Planificación y aceptación del sistema
Minimizar el riesgo de fallas de los sistemas.

10.3.1 Gestión de la capacidad.
Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema. La Oficina Asesora de Planeación y Tecnologías de la Información, con el insumo que entreguen los dueños de los diferentes Sistemas de Información, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectará las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuado, se tomará en cuenta además los

nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información para el periodo estipulado de vida útil de cada componente.

10.3.2 Aceptación del sistema.

Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación, siguiendo los lineamientos y criterios definidos en la Política de desarrollo y mantenimiento de software del Idartes.

10.4 Protección contra códigos maliciosos y móviles

Proteger la integridad del software y de la información.

10.4.1 Controles contra códigos maliciosos.

Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.

- Realizar configuraciones en la seguridad perimetral del Idartes para evitar que el software y los medios de procesamiento de la información sean vulnerables a la introducción de códigos maliciosos, tales como virus Troyanos, bombas lógicas; a través de la herramienta de antivirus que sea implementada por la Oficina Asesora de Planeación y Tecnologías de la Información.
- La Oficina Asesora de Planeación y Tecnologías de la Información definirá e implementará controles de detección y prevención para la protección contra software malicioso en las diferentes unidades de gestión de las sedes de la Entidad.
- Se desarrollarán lineamientos y actividades de sensibilización de usuarios en materia de seguridad y se definirán las pautas y los criterios para el control de acceso a los sistemas de información.
- Los controles aplicados a la seguridad de la información para protección de malware y virus deberán tener en cuenta lo siguiente:
    - Prohibir el uso de software no autorizado por la entidad.
    - Instalar y actualizar periódicamente software de detección y reparación de virus, con la finalidad de examinar computadoras y medios informáticos, como medida preventiva.
    - Capacitar a los usuarios para que puedan identificar posibles eventos de riesgo que puedan afectar la información del Idartes.

10.5 Respaldo

Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información, por esto, con el propósito de mantener la integridad y disponibilidad de la información, así como los medios tecnológicos para el procesamiento de información, se debe cumplir con el procedimiento definido de copias y respaldos para implementar los controles de respaldo acorde a la estrategia para tomar backup de los datos y practicar su restauración oportuna.

10.5.1 Respaldo de la información.

Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con procedimiento aprobado para la gestión de tecnologías de la información de la Oficina Asesora de Planeación y Tecnologías de la Información.

- La Oficina Asesora de Planeación y Tecnologías de la Información determinará sobre la base de la criticidad de la información de que se trate, un esquema de resguardo. Así mismo, dispondrá y controlará la realización de dichas copias, para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de la entidad.
- Los sistemas de resguardo deberán probarse periódicamente, asegurándose de que cumplen con los requerimientos de los planes de continuidad de la entidad.
- Se definirán lineamientos para el resguardo de la información, que deberán considerar los siguientes puntos:
    - Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
    - Asignar a la información de resguardo un nivel de protección física y ambiental, según las normas aplicables.
    - Probar periódicamente los medios de resguardo.
    - Verificar y probar periódicamente los procedimientos de restauración, garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

10.6 Gestión de la seguridad de las redes

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

10.6.1 Controles de las redes.

Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito. La Oficina Asesora de Planeación y Tecnologías de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes del Instituto Distrital de las Artes - Idartes, así como el acceso no autorizado, teniendo en cuenta los siguientes criterios

- Lineamientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias o sedes CREA diferentes al edificio principal.
- Definición de controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.

- Implementar controles especiales para mantener la disponibilidad de los servicios de red y equipos de cómputo conectados a ella.
- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura tecnológica de la entidad en sus diferentes sedes.
- Establecer las responsabilidades y procedimientos para la gestión de equipos de redes;
- Definir la responsabilidad operacional por las redes para separar de las operaciones informáticas, en donde sea apropiado;
- Aplicar loging y/o autenticación Single Sign On con instrumentos de seguimiento adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información
- Definir las actividades de gestión a coordinar estrechamente tanto para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información;
- Restringir la conexión de los sistemas a la red cuando se considere necesario.

10.6.2 Seguridad de los servicios de la red.

En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.

- Establecer la tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red;
- Definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red;
- Establecer los lineamientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.
- Para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la administración y del control de seguridad de la entidad, para ello, se cuenta con procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenden:
    - Identificar las redes y los servicios de red a los cuales se permite el acceso.
    - Definir lineamientos de autorización para determinar las personas, las redes y los servicios de red a los cuales se les otorgará el acceso.
    - Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y los servicios de red.

10.7 Manejo de los medios

Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del Idartes.

10.7.1 Gestión de los medios removibles

Se deben establecer procedimientos para la gestión de los medios removibles

- El uso de medios removibles es un requerimiento que debe ser evaluado y autorizado por el Líder de Proceso del funcionario o Contratista solicitante, toda vez que la justificación de uso tenga un sentido coherente y netamente institucional.
- Cuando se autorice el uso de medios removibles en las estaciones de trabajo del Idartes, cada vez que se conecte o lean estos medios en las estaciones de trabajo del Idartes, deberán ser escaneados obligatoriamente por el software antimalware suministrado por la Entidad, con el fin de evitar infección por malware o programas con contenido malicioso o prohibido.
- Es responsabilidad de cada Funcionario o Contratista que utilice medios removibles, tomar las medidas de resguardo necesarias sobre estos activos, con el fin de evitar accesos no autorizados, daños, perdida de información o del activo mismo.
- Ante la pérdida, extravío o robo de un medio removible, el funcionario o contratista debe informar oportunamente a través del correo soporte.sistemas@idartes.gov.co al personal de Mesa de Ayuda de acuerdo a lo indicado en el procedimiento de *Gestión de Incidentes de Seguridad de la Información*, situación que debe informar con el mayor grado de detalle, indicando la información que se perdió, si fue extraviado o robado, a su vez estos eventos se deberán manejar como incidentes de seguridad de la información.
- Al término del vínculo laboral o contractual, el Funcionario o Contratista deberá suministrar a la Oficina de Tecnología los medios removibles en los cuales gestionó información institucional para que se realice el proceso de borrado seguro.

10.7.2 Eliminación de los medios.

Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los procedimientos formales.

- Al recibir un computador los miembros del grupo de Soporte deben respaldar la información contenida en este y luego eliminar toda información que el computador contenga para, posteriormente actualizar los programas y sistema operativo y. finalmente, almacenarlo o entregarlo a el miembro correspondiente según se necesite.
- Se debe llenar un documento en la cual se señale la fecha del respaldo, el ejecutor, el computador respaldado, el nombre del servidor de almacenamiento donde fue almacenado el respaldo y el nombre de la carpeta ubicada en esa unidad.

10.7.3 Lineamientos para el manejo de la información.

Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.

- El Idartes cuenta actualmente con actividades de control que son de cumplimiento para funcionarios, contratistas y terceros para el control y manejo de la información a través del *Plan de Seguridad y Privacidad de la Información.*
- Los medios y equipos donde se almacena procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.
- La entidad establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por el Idartes, velando por la disponibilidad y confidencialidad de la información.

10.7.4 Seguridad de la documentación del sistema.
La documentación del sistema debe estar protegida contra el acceso no autorizado.

- A través de la implementación de una Arquitectura Hexagonal se realizará la estructuración de lineamientos de calidad y seguridad en materia de documentación del sistema
- Con la política de desarrollo de software se dispondrán lineamientos para la estructuración de la documentación y la organización de la misma centralizándola para la consulta, control y seguimiento del sistema
- Se generarán a través de la administración de unidades de almacenamiento unidades de gestión en la nube gestionando roles y permisos de acceso que garanticen la seguridad de la información centralizada

10.8 Intercambio de la información
Mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.

10.8.1 Políticas y procedimientos para el intercambio de información
Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.

- Se generarán documentos de acuerdos para la protección de la información intercambiada de la intercepción, copiado, modificación, dirección equivocada y destrucción.
- Se realizarán actividades de afinamiento en la seguridad perimetral para detección y protección contra el código malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas.
- Se realizará la definición del uso aceptable de los elementos de comunicación electrónicas.
- Se aplicarán configuraciones de uso seguro de comunicaciones inalámbricas.

- Se tendrá responsabilidades de funcionarios, contratistas y cualquier otro usuario de no comprometer a la entidad.
- Sensibilización al personal sobre las precauciones que deben tomar a la hora de transmitir información de la Entidad.

10.8.2 Acuerdos para el intercambio

Se deben establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas.

- La Oficina Asesora de Planeación y Tecnologías de la Información realizara la gestión de actividades para garantizar la calidad y seguridad en el intercambio de información documentando los roles, responsabilidades, acciones, sanciones y demás temas referentes a la protección de la información clasificada y reservada en el intercambio de información a través de sistemas de información, aplicaciones o aplicativos manejados por la entidad.
- La Política de desarrollo de software definirá lineamientos para el uso, modificación y gestión de la información en las actividades de intercambio a través de las diferentes modalidades contractuales legalmente definidas.
- De conformidad con el artículo 209 de la Constitución Política de Colombia, la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, y que, atendiendo a lo establecido en el artículo 113 misma normativa, los distintos órganos del Estado tienen funciones separadas, pero colaboran armónicamente y realizaran intercambio de información para la realización de sus fines.
- La información de propiedad del IDARTES, estará desarrollada u obtenida en concordancia con la Constitución Nacional y la ley, como resultado de sus procesos, programas y proyectos y, en consecuencia, comprende documentos, datos, tecnología y/o material que se puede considerar único y catalogada como pública clasificada o pública reservada de acuerdo con los artículos 18 y 19 de la Ley 1712 de 2014.
- Se aplicara a los intercambio de información lo establecido en la expedición de la Ley Estatutaria 1581 de 2012, las disposiciones generales para la protección de datos personales recolectados en bases de datos o archivos, las cuales deberán cumplirse por ambas partes, tratándolas exclusivamente para las finalidades recolectadas descritas en la Resolución 874 de 2020 de la *Política de Protección de Datos Personales del Instituto Distrital de las Artes – Idartes*, y se adoptan los formatos de autorización de tratamiento de datos personales y el aviso de privacidad definidos por la Entidad.

10.8.3 Medios físicos en tránsito.

Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.

- La Oficina Asesora de Planeación y Tecnologías de la Información realizara acciones para que se establezcan acuerdos comunes entre las organizaciones, contratistas o partes externas para el traslado de la información o equipos que contengan información institucional.
- Se establecerán los lineamientos para aplicar seguridad a los activos de información fuera de las dependencias del Idartes, considerando los distintos riesgos de trabajar fuera de la institución.
- Para el traslado o envío de medios de información fuera de las instalaciones físicas del Idartes, se debe definir en primer lugar las condiciones mínimas de seguridad que exige el activo de información
- El embalaje debe proteger el contenido de cualquier daño físico, ambiental o de otra naturaleza que pueda ocurrir durante el transporte, de acuerdo a las especificaciones definidas por el fabricante.
- En el caso de información confidencial, se debe etiquetar cómo tal y especificar claramente el destinatario.
- Cualquier violación a la seguridad establecida debe ser informada de inmediato cómo incidente de Seguridad de la Información a través de los canales establecidos para ello.

10.8.4 Mensajería electrónica.

La información contenida en la mensajería electrónica debe tener la protección adecuada, dado que la mensajería electrónica como el correo electrónico, el intercambio de datos electrónicos, las mensajerías instantáneas tienen un papel importante en las comunicaciones de la Entidad, la mensajería electrónica tiene diferentes riesgos que las comunicaciones basadas en papel, por lo tanto, se considerarán las siguientes medidas de seguridad en los mensajes electrónicos:

- Los correos electrónicos institucionales contaran con niveles altos de controles de autenticación para los accesos desde las redes accesibles.
- El correo electrónico institucional es un medio formal y oficial de comunicaciones del Idartes y una herramienta de trabajo que ha dispuesto la Entidad con el fin de facilitar las labores propias de los cargos de cada uno de sus empleados, funcionarios y contratistas; teniendo en cuenta esto, es primordial definir los lineamientos que se deben tener presente de acuerdo con las obligaciones, prohibiciones que cada empleado, funcionarios y contratistas debe tener presente.
- La Entidad en cualquier momento podrá implementar las medidas necesarias en la plataforma del correo institucional, en aras de incrementar los niveles de seguridad y/o de brindar calidad en un mejor servicio.
- Los usuarios son responsables de todas las actividades que se realicen desde su cuenta de correo institucional.
- Las cuentas de correo institucional son de uso personal e intransferible, por lo tanto, es responsabilidad del usuario salvaguardar la contraseña, cambiarla periódicamente, y no prestarla bajo ninguna circunstancia, a excepción de aquellas que sean creadas para

fines colaborativos de las unidades de gestión con la respectiva justificación y autorización.

- Las cuentas de correo institucional son creadas para el uso exclusivo de las funciones propias del usuario, por lo tanto, el usuario debe hacer uso de este servicio implementando criterios de racionalidad, respeto, responsabilidad, integridad y seguridad de la información.
- Es responsabilidad del usuario gestionar copias de seguridad de la información del correo, cuando lo considere pertinente, solicitando el correspondiente apoyo a soporte.sistemas@idartes.gov.co.
- Antes de enviar un correo electrónico, el usuario debe utilizar el corrector ortográfico de la herramienta que utilice como gestor del correo.
- Al momento de enviar información SECRETA, CONFIDENCIAL, RESTRINGIDA; se debe etiquetar como tal en el asunto del mensaje de correo electrónico que se envíe.
- El envío de correos electrónicos implica el consumo de recursos tecnológicos y demanda tiempo a la persona receptora, por tal razón se debe evitar el envío de correos innecesarios y que no guarden relación con el desempeño de las funciones asignadas a funcionarios y contratistas.
- Antes de responder o reenviar un correo, el usuario debe validar si se requiere incluir todos los destinatarios, el historial y la información que posee el mismo.
- Todo correo de procedencia desconocida, correo basura, SPAM, correo no deseado, etc. que sea recibido en los buzones de correo electrónico del Idartes, debe ser ignorado, eliminado inmediatamente y reportado a la Mesa de ayuda por los canales establecidos con el fin de evitar posibles infecciones por código malicioso o virus.
- El usuario del correo electrónico se compromete a reportar oportunamente a la Mesa de Ayuda cualquier fallo de seguridad de su cuenta institucional, incluyendo el uso no autorizado, perdida de contraseñas, etc.
- Según lo establecido en la Ley 524 de 1999, los mensajes de correo electrónico revisten la misma fuerza probatoria que tienen los documentos físicos.
- El correo electrónico institucional es una herramienta de trabajo, de uso exclusivamente laboral, por tanto, la información contenida en estos es de propiedad de la Entidad. En esa medida, la Entidad no se hace responsable de la información de carácter personal que los usuarios almacenen en las cuentas institucionales.
- En caso de que se requiera el funcionamiento de una sola cuenta de correo para dos o más usuarios, el usuario principal y dueño de la cuenta de correo debe otorgar dicha autorización por escrito o por correo electrónico indicando que usuarios tendrán acceso a la cuenta de correo, y en todo caso dicha autorización no exime de toda
- responsabilidad al usuario dueño de la cuenta del correo uso de la cuenta y de los lineamientos planteados en el presente documento.
- Se recomienda hacer caso omiso a los links que vengan agregados en el cuerpo del correo de cuentas externas; por lo tanto, se aconseja digitar directamente la página que deseen consultar en el navegador del equipo

- El envío de correos con mensajes que contravengan las normas legales, la moral, el orden público, la intimidad o el bueno nombre de las personas, que contengan contenido irrespetuoso, difamatorio, racista, religioso irrespetuoso, discriminatorio, de acoso o intimidación; así como imágenes o videos con contenidos ilegales, ofensivo, extorsivo, indecente o con material sexual.
- Al ser el correo electrónico institucional la herramienta dispuesta por el Idartes como medio de comunicación oficial, se prohíbe el uso de correos personales con el fin de establecer o transferir información institucional.
- El uso no adecuado o incumplimiento de las medidas definidas en el uso del correo institucional, da lugar a la aplicación de las medidas administrativas, disciplinarias o legales a que haya lugar.

10.8.5 Sistemas de información del negocio.

Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información.

- La Oficina Asesora de Planeación y Tecnologías de la Información realizará la actualización de los procedimientos referentes a la gestión de desarrollo y mantenimiento de software donde definirá lineamientos para la interconexión de los sistemas de información en materia de seguridad y calidad de la información.
- Se definiera y mantendrá actualizada la política de desarrollo de software en cabeza de la Oficina Asesora de Planeación y Tecnologías de la Información con las correspondientes actualizaciones a lugar respecto a la normativa vigente en materia de desarrollo y mantenimiento de software.

10.9 Servicios de comercio electrónico

Garantizar la seguridad de los servicios de comercio electrónico, y su utilización segura.

10.9.1 Comercio electrónico

La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.

- La Oficina Asesora de Planeación y Tecnologías de la Información realizara configuraciones en los sistemas de información que involucran transacciones de comercio electrónico con el fin de aplicar validación de acceso con credenciales para os usuarios que garanticen la seguridad y el no repudio de la información que se tramite a través de las redes de conectividad dispuestas para tal fin.
- La Oficina Asesora de Planeación y Tecnologías de la Información realizara la configuración de servidor seguro de páginas web con certificados SSL que establecen una conexión cifrada con el cliente que ha solicitado la conexión, de manera que nadie, salvo el servidor y el cliente, puedan tener acceso a la información transmitida.

10.9.2 Transacciones en línea

La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.

- Para las transacciones en línea se dispondrá de medios de validación de seguridad digital para las firmas de autorizaciones y aprobaciones
- Para las transacciones se utilizarán páginas con certificados SSL que contengan un protocolo de intercambio de información que permite asegurar la autentificación, confidencialidad e integridad de los datos que se transmiten a través de Internet.
- Para las transacciones comerciales se usarán sistemas de criptografía asimétrica están basados en el cifrado de la información a partir de un par de claves diferentes, denominadas pública y privada, que se atribuyen a una persona determinada.

10.9.3 Información disponible al público

La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.

- Para la información disponible se debe ofrecer información clara y concisa sobre los productos y sus condiciones.
- Usar un servidor seguro para alojar las páginas transaccionales de información.
- Aplicar configuración de seguridad al servidor del comercio para aumentar la confianza y seguridad de los usuarios en el manejo de la información.
- Definir la privacidad de los datos del usuario y solicitar sólo los datos necesarios.

10.10 Monitoreo

Detectar actividades de procesamiento de la información no autorizadas.

10.10.1 Protección de la información del registro

Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.

- La Oficina Asesora de Planeación y Tecnologías de la Información dispondrá de espacios adecuados para el procesamientos, control y seguimiento de servicios e información que estén protegidos contra accesos físicos y lógicos no autorizados

10.10.2 Registros del administrador y del operador

Se deben registrar las actividades tanto del operador como del administrador del sistema.

- Los titulares de cuenta de usuario privilegiado pueden estar en capacidad de manipular los logs en instalaciones de procesamiento de información bajo su control directo; por esto, es necesario proteger y revisar los logs para mantener la rendición de cuentas para los usuarios privilegiados.

10.10.3 Registro de fallas

Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.

- Se deben monitorear los sistemas y se deben reportar los eventos de seguridad de la información utilizando documentos de seguimiento de registro de las fallas definidos por la Oficina Asesora de Planeación y Tecnologías de la Información para asegurar que se identifiquen los problemas en los sistemas de información

10.10.4 Sincronización de relojes

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.

- Se realizará la configuración de relojes en los servidores de re con el ajuste correcto de los relojes de computador para asegurar la exactitud de los logs de auditoría
- Los logs con el reloj sincronizado desde el servidor se pueden usar en caso de ser necesarios para investigaciones o como evidencia legal en casos legales o casos disciplinarios.
- Un reloj vinculado a una transmisión de tiempo por radio desde un reloj atómico nacional se puede usar como el reloj maestro para los sistemas de loging.
- Se puede usar un protocolo de tiempo de red para mantener todos los servidores sincronizados con el reloj maestro en el servidor de red principal.

11 CONTROL DE ACCESO

11.1 Requisito del negocio para el control de acceso

Controlar el acceso a la información.

11.1.1 lineamientos de control de acceso

Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso. En la aplicación de gestión de accesos, se tendrán en cuenta los siguientes aspectos:

- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones.
- Identificar la normatividad aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo y/o de acuerdo con sus obligaciones contractuales
- Toda actividad que requiera acceder a los servidores, equipos o a las redes del Idartes, se debe realizar en las instalaciones. No se debe realizar ninguna actividad de tipo

remoto exceptuando las que tengan la debida autorización la Oficina Asesora de Planeación y Tecnologías de la Información.
- La conexión remota a la red de área local del Idartes debe ser establecida a través de una conexión VPN segura aprovisionada por la entidad, la cual debe ser autorizada por la Oficina Asesora de Planeación y Tecnologías de la Información, que cuenta con el monitoreo y registro de las actividades necesarias.

11.2 Gestión del acceso de usuarios

Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

11.2.1 Registro de usuarios.

Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.

- Uso de identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo usuario. El uso de identificadores grupales solo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- Verificación de la autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- Verificación del nivel de acceso otorgado coherente con la Política de Seguridad de la Información de la entidad
- Mantenimiento de un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelación inmediatamente de los derechos de acceso para los usuarios que cambiaron sus tareas o de aquellos a los que se les revocó la autorización, se desvincularon de la entidad o sufrieron la pérdida de sus credenciales de acceso
- Cada uno de los procesos de la Entidad es responsable de comunicar a la Oficina de Talento Humano y/o de Gestión Contractual, el cambio de cargo, funciones o actividades o la terminación contractual de los Colaboradores pertenecientes al proceso funcionarios y/o contratistas, y los líderes de la Gestión Contractual son las encargadas de comunicar a la Oficina Asesora de Planeación y Tecnologías de la Información sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

11.2.2 Gestión de privilegios.

Se debe restringir y controlar la asignación y uso de privilegios.

- Para solicitudes masivas (3 o más personas) de creación de usuario de red, correo electrónico, sistemas de información, etc. se deberá descargar el formato para solicitud masiva de creación de creación de usuarios (archivo.xlsx), en la sección mapa de

procesos, diligenciar todos sus campos, y nuevamente ser cargado al sitio web destinado para tal fin o enviarse al correo soporte.sistemas@idartes.gov.co.

- Las solicitudes de creación de usuario de red, correo electrónico, sistemas de información, etc. para personal de planta serán realizadas por el Área de Talento Humano, y para el caso de los Contratistas será responsabilidad del jefe de Área, Gerente, subdirector o una persona quien sea designada por escrito al correo soporte.sistemas@idartes.gov.co para dicha actividad.
- En situaciones especiales como permisos, incapacidades, adición de contrato, suspensión, reactivación o terminación anticipada de contrato o retiro del personal, será responsabilidad del Jefe de Área, Gerente, Subdirector o una persona quien sea designada por escrito al correo soporte.sistemas@idartes.gov.co para dicha actividad, informar la novedad enviando la solicitud de actualización de la información a la Oficina Asesora de Planeación y Tecnologías de la Información través del formulario y será registrado automáticamente en la herramienta de mesa de ayuda de la Entidad.

11.2.3 Gestión de contraseñas para usuarios.

La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.

- Se establece el uso de contraseñas individuales para determinar las responsabilidades de su administración.
- Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire.
- Las contraseñas deben contener Mayúsculas, Minúsculas, números y por lo menos un carácter especial y de una longitud mayor a 8 caracteres.
- Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.
- Cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware como servidores, impresoras, routers, switch y herramientas de seguridad perimetral.
- No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, Jefes u otras personas que lo soliciten.
- Todos los usuarios deben dar cumplimiento a las políticas de seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

11.2.4 Revisión de los derechos de acceso de los usuarios.

La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.

- Los derechos de acceso de los usuarios a la información y a la Plataforma Tecnológica y de procesamiento de información del Idartes, debe ser revisada periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.

11.3 Responsabilidades de los usuarios

Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.

11.3.1 Uso de contraseñas.

Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.

- Se debe identificar y autenticar a cualquier usuario que, de manera local o remota, requiera utilizar los recursos tecnológicos del Instituto Distrital de las Artes - Idartes, para lo cual se requiere contar con sistemas de seguridad que cumplan al menos con las siguientes características:
  - Cada usuario que requiera acceder a la plataforma tiene que identificarse y autenticarse antes de acceder a un recurso tecnológico a través de un usuario y una contraseña, y el usuario debe estar activo.
  - Una vez se han identificado y autenticado, los usuarios sólo podrán acceder a los recursos sobre los cuales están autorizados.
  - Debe quedar registro de los eventos de ingreso y autenticación de usuarios, para monitoreo de la Oficina Asesora de Planeación y Tecnologías de la Información.

- El usuario deberá realizar todas las medidas a su alcance para evitar el acceso de usuarios no autorizados, evitar poner en peligro la información del Instituto Distrital de las Artes - Idartes. El compromiso de los usuarios autorizados es fundamental para una seguridad efectiva. Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario.
- Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, que constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a los servicios tecnológicos y de manejo de información de la entidad.
- Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se podrá utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.
- Se realizará la verificación del nivel de acceso otorgado coherente con la *Plan de Seguridad y Privacidad de la Información* de la entidad

11.3.2 Equipo de usuario desatendido.

Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.

- Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

- Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.
- La Oficina Asesora de Planeación y Tecnologías de la Información debe coordinar las tareas de sensibilización a todos los usuarios charlas de capacitación, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación con la implementación de dicha protección.
- Se deben cerrar las sesiones activas cuando hayan terminado, a menos que se puedan asegurar mediante un mecanismo de bloqueo apropiado, como un protector de pantalla protegido con contraseña;
- Se debe realizar una salida segura del sistema para salir de las aplicaciones o servicios de red cuando ya no los necesiten;
- Asegurar que los computadores o dispositivos móviles contra uso no autorizado mediante el bloqueo de teclas o un control equivalente como acceso con contraseña, y cuando no están en uso.

11.3.3 Lineamientos de escritorio despejado y de pantalla despejada

Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.

- Todo el personal del Idartes debe conservar su escritorio libre de información propia de la entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.
- Todo el personal del Idartes debe bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de ellos o que por cualquier motivo deban dejar su puesto de trabajo.
- Todos los usuarios al finalizar sus actividades diarias deben salir de todas las aplicaciones y apagar las estaciones de trabajo.
- Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. No se deben reutilizar papel que contenga información CONFIDENCIAL.
- En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios deben dejar la información CONFIDENCIAL protegida.
  Almacenar con el debido resguardo y cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes u otro tipo de mobiliario seguro, cuando no están siendo utilizados, especialmente fuera del horario de trabajo y teniendo en cuenta lo establecido en el procedimiento correspondiente a la gestión documental

11.4 Control de acceso a las redes

Evitar el acceso no autorizado a servicios en red.

11.4.1 Política de uso de los servicios de red.

Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.

- las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la administración y del control de seguridad de la entidad, para ello, se cuenta con procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenden:
  - Identificar las redes y los servicios de red a los cuales se permite el acceso.
  - Definir lineamientos de autorización para determinar las personas, las redes y los servicios de red a los cuales se les otorgará el acceso.
  - Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y los servicios de red.
- El servicio institucional de Internet se constituye en una herramienta tecnológica que facilita el cumplimiento de las funciones y responsabilidades de los servidores de la Institución, funcionarios, contratistas, terceros y/o pasantes autorizados, dentro de los procesos institucionales.
- Se considera como uso aceptable del servicio institucional de Internet, la navegación para realizar tareas y actividades relacionadas a las funciones asignadas a los servidores de la Institución, siempre y cuando estén involucrados dentro de los procesos institucionales.
- El grupo de Redes e Infraestructura administrará el servicio institucional de Internet y red LAN, así mismo, otorgará accesos a los usuarios solicitantes de este servicio.
- Todos los computadores de escritorio y/o portátiles asignados a los servidores de la Institución, funcionarios, personal externo, terceros y/o contratistas autorizados al uso del Servicio Institucional de Internet, deberán tener instalado y operativo el antivirus para protegerlo contra amenazas de malware o código malicioso.
- El grupo de Redes e Infraestructura es responsable de implementar las herramientas informáticas que permitan la administración del servicio Institucional de Internet, y minimizar los riesgos que afecten a la continuidad del servicio.

11.4.2 Autenticación de usuarios para conexiones externas.

Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.

- La autenticación es una manera de restringir el acceso a usuarios específicos cuando acceden a un sistema remoto. La autenticación se puede configurar en el nivel del sistema y en el nivel de red.
- Después de que un usuario haya obtenido acceso a un sistema remoto, la autorización es una manera de limitar las operaciones que el usuario puede realizar
- Se crearán políticas de firewall para dar acceso a recursos específicos de red a usuarios y grupos en los ambientes de red donde varios usuarios comparten direccionamiento IP.

11.4.6 Control de conexión a las redes.

Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso.

- El acceso remoto a los servidores críticos y bases de datos, se realizan por el líder, administrador de TI.
- Se debe tener implementado como múltiple factor de autenticación aplicaciones del dispositivo de la entidad o de terceros que se conecte, mediante la cual se accederá a la plataforma tecnológica del Idartes.
- Se establece el tiempo de desconexión por inactividad de la sesión es de 10 minutos.
- El oficial de seguridad autoriza los accesos remotos de los empleados y proveedores.
- Está prohibido copiar, mover o almacenar información de las bases de datos de los servidores cuando se acceda mediante tecnologías de acceso remoto.
- La infraestructura del Idartes deberá estar separada por Vlans para garantizar la confidencialidad de los datos que se transmitan

11.4.7 Control de enrutamiento en la red.

Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio.

- El grupo de redes de la Oficina Asesora de Planeación y Tecnologías de la Información debe realizar segmentación de Redes y enrutamiento para servidores públicos, contratistas y visitantes del Idartes, se debe establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
- Se debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación o enrutamiento que se considere conveniente para la Entidad.
- Se debe instalar protección entre el enrutamiento de las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración de la Entidad

11.5 Control de acceso al sistema operativo

Evitar el acceso no autorizado a los sistemas operativos.

11.5.1 Procedimientos de ingreso seguros

El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.

- Se debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado. Adicionalmente, el procedimiento de identificación deberá tener en cuenta los siguientes aspectos:
    - Mantener en secreto los identificadores de sistemas o aplicaciones, hasta tanto se haya llevado a cabo exitosamente el proceso de conexión.
    - Desplegar un aviso general advirtiendo que solo los usuarios autorizados pueden acceder al equipo de cómputo.
    - Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
    - Validar la información de la conexión solo al completarse la totalidad de los datos de entrada.
    - Limitar el número de intentos de conexión no exitosos permitidos y registrar los intentos no exitosos.
    - Impedir otros intentos de identificación, una vez superado el límite permitido.
- En caso de corresponder, la Oficina Asesora de Planeación y Tecnologías de la Información en conjunto con los Propietarios de la Información deberán definir cuales se consideran terminales de alto riesgo, por ejemplo, áreas públicas o externas fuera del alcance de la gestión de seguridad de la entidad, o que sirven a sistemas de alto riesgo, estas se apagarán después de un periodo definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas.

11.5.2 Identificación y autenticación de usuarios.

Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.

- Las cuentas de usuario tienen dos partes, un nombre de usuario y una contraseña, cada usuario autenticado está asociado a una dirección IP
- La combinación de nombre de usuario, contraseña y dirección IP permitirá al administrador del dispositivo monitorear las conexiones a través del dispositivo.
- Con la autenticación, los usuarios pueden iniciar sesión en la red desde cualquier equipo, pero acceder sólo a los protocolos y puertos de red a los cuales estén autorizados.
- Identificar las conexiones que se inician desde una dirección IP determinada y también transmitir el nombre de la sesión mientras el usuario está autenticado.

11.5.3 Sistema de gestión de contraseñas.

Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.

- El acceso a información restringida debe estar controlado, se aplicará en equipos de cómputo del Idartes el uso de sistemas automatizados de autenticación que manejen credenciales.

- Corresponde a la Oficina Asesora de Planeación y Tecnologías de la Información elaborar, mantener y publicar los documentos de gestión de red que ofrece la institución a su personal, funcionarios y contratistas.
- La Oficina Asesora de Planeación y Tecnologías de la Información debe elaborar, mantener y publicar procedimientos de *gestión de cuentas de usuario* para el uso de servicios de red.
- Las claves de administrador de los sistemas deben ser conservadas por la Oficina Asesora de Planeación y Tecnologías de la Información y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie, se exceptúa de lo anterior las claves de administrador de servidores y equipos de escritorio adscritos al grupo de redes las cuales deben ser conservadas y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo considere necesario el cambio.
- La Red de Datos del Idartes en coordinación con el grupo de tecnología deben elaborar, mantener y actualizar los procedimientos sobre la gestión de usuarios y las guías para la correcta definición, uso y complejidad de claves de usuario.

11.5.4 Uso de las utilidades del sistema

Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.

- El acceso a sistemas de cómputo, a las aplicaciones, utilidades y los datos que contienen es responsabilidad exclusiva del personal encargado de tales sistemas.
- El Idartes a través del grupo de tecnología gestionará las cuentas de usuarios y los permisos de acceso para mantener al mínimo la cantidad de cuentas de usuario que el personal, funcionarios, contratistas y terceros deben poseer para acceder a los servicios de red y utilidades del sistema.
- El control de las contraseñas de red y uso de equipos es responsabilidad de la Red de Datos del Idartes, las contraseñas deben ser codificadas y almacenadas de forma segura permitiendo que el uso de las utilidades del sistema sea seguro.

11.5.5 Tiempo de inactividad de la sesión

Las sesiones inactivas se deben suspender después de un periodo definido de inactividad.

- Aplicar una herramienta de desconexión por tiempo muerto, que deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red.
- El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.
- Se debe implementar la desconexión por tiempo muerto en las conexiones remotas, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

- Si un usuario debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

11.6 Control de acceso a las aplicaciones y a la información
Evitar el acceso no autorizado a la información contenida en los sistemas de información.

11.6.1 Restricción de acceso a la información.
Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.

- El acceso a información restringida debe estar controlado, se aplicará en equipos de cómputo del Idartes el uso de sistemas automatizados de autenticación que manejen credenciales.
- Con la autenticación, los usuarios pueden iniciar sesión en la red desde cualquier equipo, pero acceder sólo a los protocolos y puertos de red a los cuales estén autorizados.
- Incluso cuando un usuario tenga un permiso de acceso y una contraseña válida a un sistema, la Oficina Asesora de Planeación y Tecnologías de la Información validara los roles para que solo se asigne el acceso necesario a la información contenida en el sistema que requiera para el desempeño de las actividades del vínculo laboral.

11.6.2 Aislamiento de sistemas sensibles.
Los sistemas sensibles deben tener un entorno informático dedicado (aislados).

- Evitar el acceso no autorizado es la de limitar los lugares en los cuales se almacena o procesa la información.
- En los sistemas de cómputo en red, es recomendable mantener toda la información, especialmente la sensible, en servidores centralizados y no en el disco duro de las computadoras personales.

11.7 Computación móvil y trabajo remoto
Garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.

11.7.1 Computación y comunicaciones móviles.
Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

- Definir procedimientos que permitan al poseedor del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran

expuestos la información y los sistemas de información de la entidad, los que deberán incluir:
    - Revocación de las credenciales afectadas
    - Notificación a grupos de trabajo donde potencialmente se pudieran haber comprometido recursos.
- La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto, en consecuencia, debe entrenarse especialmente al personal que los utilice.
- Tener un antivirus instalado en los dispositivos
- Revisar las fuentes de donde se realizan descargas de aplicaciones
- Revisar constantemente los permisos que solicitan las aplicaciones

11.7.2 Trabajo remoto.

Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

- El trabajo remoto sólo podrá ser autorizado y definido por el Director o Jefe de Dependencia a la cual pertenezca el usuario solicitante, previa aprobación Talento Humano, y apoyado por la Oficina Asesora de Planeación y Tecnologías de la Información, quien determinará las medidas que correspondan en materia de seguridad de la información, con el fin de garantizar el cumplimiento de esta Política, los lineamientos, normas y procedimientos existentes.

- Toda información gestionada por la entidad, y que sea accedida remotamente en modalidad de teletrabajo, debe ser utilizada únicamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales de esta.
- La Entidad brinda los lineamientos de seguridad digital para la protección de la información a la que se tiene acceso, se procesa y almacena en lugares en los que se realiza teletrabajo o trabajo remoto, y se hace uso de los recursos tecnológicos autorizados por la Entidad para el desarrollo de las actividades de teletrabajo o trabajo remoto.
- La Entidad establece los requerimientos para la autorización de conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de Idartes, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.
- La entidad establece el proceso de implementación de teletrabajo, de acuerdo con la normativa y los lineamientos exigidos, con el fin de proteger la información.
- La Entidad es la encargada de velar por la seguridad física del entorno del sitio donde se van a realizar actividades de teletrabajo, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.

12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

12.1 Requisitos de seguridad de los sistemas de información

Garantizar que la seguridad es parte integral de los sistemas de información.

12.1.1 Análisis y especificación de los requisitos de seguridad

Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.

- La arquitectura de software debe describir la manera en que el sistema de información maneja aspectos como
- seguridad, comunicación entre componentes, formato de los datos, acceso a fuentes de datos, entre otros.
- La Oficina Asesora de Planeación y Tecnologías de la Información mantendrá actualizada la *Política de Desarrollo de Software* con los respectivos lineamientos de cara a los sistemas de información del Idartes.
- Cada característica de la arquitectura definida para la gestión de desarrollo con los atributos de calidad, es una propiedad medible del sistema que permite evaluar aspectos de calidad tales como la disponibilidad, capacidad de mantenimiento, eficiencia, funcionalidad, seguridad, usabilidad, escalabilidad, facilidad de pruebas, despliegue y desarrollo.

12.2 Procesamiento correcto en las aplicaciones

Evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

12.2.1 Validación de los datos de entrada y salida.

Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados

- Los requisitos de seguridad deberían ser identificados y consensuados antes de desarrollar los sistemas de información aplicando los siguientes criterios de seguridad:
- Detectar características inválidas, datos incompletos e inconsistentes
- Para que todo ande bien se tiene que realizar una revisión periódica para poder confirmar la integridad es decir se debe monitorear en constantemente.
- Definición de las responsabilidades de todos los implicados, dado que es importante establecer las responsabilidades que corresponden, y las capacidades y aptitudes que deben contar las personas que los utilicen para no incurrir en errores.
- A través de lineamientos del grupo de desarrollo se incorporarán verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.

- El grupo de desarrollo de la Oficina Asesora de Planeación y Tecnologías de la Información definirá y aplicará lineamientos para identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.
- Se darán lineamientos por parte del grupo de desarrollo para validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias

12.3 Controles criptográficos

Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.

12.3.1 Política sobre el uso de controles criptográficos.

Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

- El responsable de Gestión de Seguridad, en conjunto con el líder responsable del desarrollo, y el líder de infraestructura o administrador networking, definirán el proceso administrativo de claves, así como la administración de las técnicas criptográficas que deban utilizarse.
- Se definirá y aplicará el uso de técnicas criptográficas para proteger la confidencialidad, integridad y la autenticidad de la información, para unidades de gestión con información que requiera conforme a sus responsabilidades mayor seguridad
- La Oficina Asesora de Planeación y Tecnologías de la Información debe verificar que todo sistema de información que requiera realizar transmisión de información clasificada o reservada cuente con mecanismos de cifrado de datos.
- La Oficina Asesora de Planeación y Tecnologías de la Información debe, en cabeza de los proveedores de desarrollado de software deben asegurar que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por el Idartes.

12.3.2 Gestión de llaves.

Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.

- La Oficina Asesora de Planeación y Tecnologías de la Información establece los lineamientos necesarios para el control y el uso de las firmas digitales para el Idartes.
- Toda solicitud de asignación de firma digital se realiza a través de la mesa de ayuda del Idartes.
- Los servidores públicos y contratistas deben firmar documentos que permitan establecer un acuerdo sobre uso del mecanismo de firma digital

- Los servidores públicos y contratistas, que realicen actividades para el Idartes, y tengan a su cargo una firma digital, deben hacer buen uso de esta de acuerdo a los lineamientos establecidos.
- Los Servidores Públicos y contratistas que se les haya asignado firma digital, deben hacer uso de esta para el desarrollo de sus actividades, así mismo gestionar la renovación del certificado de la firma, cuando esté próxima a vencer.
- Todos los documentos firmados digitalmente son auténticos se tomarán como originales y finales, dado que por medio de esta validación de identidad se cumplen con los criterios de seguridad de la información de integridad, confidencialidad, y disponibilidad.

12.4 Seguridad de los archivos del sistema
Garantizar la seguridad de los archivos del sistema.

12.4.1 Control del software operativo.
Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

12.4.2 Protección de los datos de prueba del sistema.
Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse

12.4.3 Control de acceso al código fuente de los programas
Se debe restringir el acceso al código fuente de los programas.

12.5 Seguridad en los procesos de desarrollo y soporte
mantener la seguridad del software y de la información del sistema de aplicaciones.

12.5.1 Procedimientos de control de cambios.
Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.

- Mantener actualizadas las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios.
- llevar una trazabilidad del control de cambios solicitados y realizados sobre el software y sistemas de información del Idartes.
- Se debe establecer y aplicar el lineamiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware.
- Se deben especificar en qué momento existen cambios de emergencia en la cual se debe garantizar que los cambios se apliquen de forma rápida y controlada.
- Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa

y se debe involucrar e informar a los Colaboradores o Terceros que por sus funciones tienen relación con el sistema de información.
- Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.

12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.
Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

- Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente.

12.5.3 Restricciones en los cambios a los paquetes de software.
Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente. En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del responsable del activo de información y el Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información se debe:

- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- Evaluar el impacto que se produce si el Ministerio se hace cargo del mantenimiento.
- Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

12.6 Gestión de la vulnerabilidad técnica
Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

12.6.1 Control de vulnerabilidades técnicas
Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

- Documentar y Mapear los datos de los sistemas de información identificando características de tamaño del sistema, infraestructura general, aplicaciones financieras, dispositivos utilizados, lugares de almacenamiento de datos, fabricantes del software, versiones utilizadas, lugar de instalación y responsables directos.

- Establecer los roles y responsables en la gestión de vulnerabilidades para asegurar su eficacia operativa y analítica. Identificar los riesgos de los datos y sus ramificaciones, virtuales o analógicos, recopilando información para identificar sus influencias directas e indirectas.
- Resguardar los datos sensibles con la seguridad definida para garantizar la seguridad, la estabilidad y supervivencia estratégica y comercial del Idartes.
- Analizar el escenario y definir las prioridades, conforme a este análisis de los riesgos se establece prioridades para los planes de gestión de vulnerabilidades que deban estructurarse.
- Usar informes como táctica estratégica para garantizar la medición del progreso de las operaciones de gestión de vulnerabilidades.
- Adoptar métricas inteligentes puede facilitar el análisis y optimizar la toma de decisiones.
- Corregir las vulnerabilidades de forma estructurada, bajo lineamientos del equipo de desarrollo para cada caso en específico.

13 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información

Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

13.1.1 Reporte sobre los eventos de seguridad de la información

Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.

- Aplicar un modelo técnico de gestión de incidentes de seguridad de la información se involucran las siguientes fases de manera cíclica:
  - Preparación, reporte y registro de eventos e incidentes
  - Detección y análisis.
  - Contención, erradicación, recuperación y respuesta.
  - Actividades Post-Incidentes.
- Todos los incidentes de seguridad deberán estar registrados en la herramienta de gestión de mesa de ayuda con los canales que sean establecidos por el Idartes.

13.1.2 Reporte sobre las debilidades de la seguridad

Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

- De acuerdo con el *Plan de seguridad y privacidad de la información,* es responsabilidad de todos los funcionarios, terceros y contratistas que tengan acceso a los activos de

información del Idartes reportar a la mesa de ayuda, los eventos tecnológicos o incidentes de seguridad de la información

- El equipo de soporte y mesa de ayuda debe realizar el registro de los eventos tecnológicos o incidentes de seguridad de la información que reporte los funcionarios, en la herramienta de mesa de ayuda de la Entidad, teniendo en cuenta que el o los administradores de la herramienta definida deben mantenerla activa y configurada para el registro de los eventos tecnológicos o incidentes de seguridad de la información, y para la emisión de los informes que se requieran.

13.2 Gestión de los incidentes y las mejoras en la seguridad de la información

Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

13.2.1 Responsabilidades y procedimientos

Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

- Una vez se reciba el reporte del posible Incidente de seguridad, la mesa de servicio debe realizar la primera categorización en la herramienta que se maneja para iniciar con la atención de este, allí se generará un ticket de servicio para la atención del caso.
- Clasificar el incidente de seguridad de acuerdo con su impacto y urgencia en la herramienta de gestión con la que cuenta el Instituto con el fin de permitir una atención adecuada a los incidentes
- Realizar el análisis, contención y erradicación, determinando el nivel de prioridad de este, y de esta manera atenderlos adecuadamente según la necesidad.
- De acuerdo a la criticidad del incidente se conformarán equipos gestión que podrán solicitar información o la participación de otros colaboradores, procesos, especialistas y/o operadores estratégicos requeridos para la atención del incidente de seguridad.
- En caso que un incidente de seguridad de la información se considere CATASTRÓFICO, se deberá informar al Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información, de la ocurrencia de dicho evento, quien deberá informar a la alta gerencia para la instalación de la mesa de crisis, en donde se analizará los recursos financieros, humanos y tecnológicos correspondientes a la atención de la emergencia, al igual evaluar las alternativas para la contención, erradicación y solución del incidente, a través de la activación del Plan de continuidad de la Operación del Idartes.
- En caso de que se presente un incidente de seguridad relacionados con base de datos que contenga información sensible, deberá ser revisado con el apoyo del oficial de datos personales del Instituto Distrital de las Artes - Idartes.
- En caso de que se presente un incidente de seguridad de la información el Director General o a quien este delegue por escrito, será el único autorizado para reportar incidentes de seguridad a los entes externos de ser necesario, si el Idartes no cuenta con los recursos necesarios y personal capacitado se debe recurrir a las entidades externas como CSIRT o ColCERT.

13.2.2 Aprendizaje debido a los incidentes de seguridad de la información

Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

- De acuerdo con la categoría del incidente de seguridad de la información, se realiza el tratamiento del mismo teniendo en cuenta la gestión de conocimiento de incidentes que ya se hayan presentado o se puede tener en cuenta lo de acuerdo a lo establecido en el Plan de Contingencia de Tecnología de la Información definido por el Idartes.
- El profesional de la seguridad de la información del Idartes dará a conocer en un informe del tratamiento y gestión del incidente de seguridad, el cual se aportará al Ticket en la herramienta de mesa de ayuda de la entidad para consulta del personal que apoya las gestiones de activos de información y riesgos de seguridad de la información con el fin de que se realicen los ajustes necesarios en cada una de sus gestiones.
- El profesional que apoya la gestión de incidentes de seguridad de la información informará las lecciones aprendidas al profesional del grupo de tecnología que apoya la gestión de cambio y cultura del equipo de seguridad de la información con el fin de fortalecer e interiorizar mediante diferentes estrategias generando conciencia en los colaboradores.
- Conforme a la documentación y solución del incidente de seguridad y privacidad de la información documentado y soportado en el Ticket registrado en la herramienta de mesa de ayuda de la entidad, se Informará o notificará a los afectados sobre incidentes que afectaron la confidencialidad o integridad de su información, así como de las medidas adoptadas para la solución del incidente.

A.13.2.3 Recolección de evidencia Control

Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

- Se deben conservar las evidencias recopiladas, con el fin de reducir la probabilidad de que estas se modifiquen después y sean consideradas no admisibles ante un ente judicial.
- Dependiendo de la evidencia que se genere en el tratamiento del incidente, se determinará el lugar en donde se conservaran las evidencias producto de un incidente de seguridad de la información asociado a un ataque informático como los *logs* de auditoría se almacenarán en un repositorio, el cual deberá cumplir unos requisitos mínimos de seguridad, los cuales se determinarán de acuerdo con la clasificación de la información para garantizar la integridad, disponibilidad y confidencialidad de la información.
- Para la adquisición, contención y preservación de la información que pueda servir como evidencia, se puede tomar como referencia los documentos internos, la ISO/IEC 27037

y 27001, la Gestión y Clasificación de Incidentes de Seguridad de la Información del MINTIC y documentos de uso libre por parte del NIST.

14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

- La Oficina Asesora de Planeación y Tecnologías de la Información debe establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación TI en caso de situaciones adversas, como desastres naturales o crisis.
- Implementar un centro de datos alterno, para garantizar la disponibilidad de los servicios críticos de la Entidad, teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en este documento.
- El Idartes cuenta con un *Plan de continuidad* que asegura la continuidad de las operaciones tecnológicas de sus procesos críticos, teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en este documento.
- El plan de continuidad adquiere mayor relevancia una vez sea apropiado por todos los Servidores Públicos de manera anticipada y será actualizado y comunicado en cada vigencia según las necesidades de la Entidad.

14.1.2 continuidad del negocio y evaluación de riesgos

Se deben identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

- Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones y responsabilidades relacionados con el plan, deben estar incorporados y definidos en los Planes de contingencia que realicen las unidades de gestión del Idartes.
- Para el monitoreo preventivo del ejercicio de continuidad del negocio y del servicio Idartes tendrá en cuenta los riesgos analizados con las diferentes unidades de gestión.

14.1.3 Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información

Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio.

- Se debe establecer un plan de pruebas periódico del plan de Contingencia de la Plataforma Tecnológica del Idartes.
- Contar con una herramienta documental que de lineamientos para gestionar y/o reaccionar adecuadamente ante posibles incidentes que pongan en riesgo a los Servidores Públicos y la plataforma tecnológica, que se pueda afectar el debido desarrollo de las actividades propias de Función Pública, impedir la prestación y continuidad del servicio a los Grupos de Valor o el cumplimiento de los compromisos establecidos en la planeación estratégica

14.1.4 Estructura para la planificación de la continuidad del negocio

Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento

- Elaborar guías de trabajo o documentos técnicos que define los elementos críticos a controlar a partir del análisis de los riesgos asociados, los responsables, etapas, definiciones y generalidades; las actividades específicas y secuenciales, fechas de ejecución, recursos requeridos como humanos, físicos, tecnológicos, económicos y el análisis de cada una de ellas

14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio

Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

- La Oficina Asesora de Planeación y Tecnologías de la Información será la encargada de aprobará y monitoreará el plan de continuidad de tecnología; las acciones preventivas se llevarán a cabo en toda la entidad según la planificación de las dependencias relacionadas con las personas, relacionadas con la infraestructura y de gestión documental relacionadas con la información; las cuales estarán coordinadas por la Oficina de Tecnologías de la Información y las Comunicaciones en lo relacionado con la infraestructura tecnológica y la seguridad de la información
- Durante la definición de la planificación institucional se definirán y aprobarán las pruebas, interrupción del servicio, evacuación de emergencia o pruebas aleatorias del plan de continuidad, según los recursos con los que se cuente, los cuales se harán de manera planificada y concertada

- Los resultados y el seguimiento se socializarán en el Comité Institucional con el personal pertinente administrativo y con los Directivos

15 CUMPLIMIENTO

15.1 Cumplimiento de los requisitos legales

Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.

15.1.1 Identificación de la legislación aplicable.

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización

- Tanto el diseño, como el funcionamiento, uso y gestión de la Seguridad de la Información pueden encontrase sujetos a los requisitos legales o a los reglamentos contractuales de seguridad.
- Los requisitos concernientes, tanto los requisitos legales como los reglamentos contractuales y el enfoque seguido por la organización para cumplirlos, deben encontrase definidos explícitamente, estar documentados y mantenerse actualizados en cada gestión de Seguridad de la Información según la normatividad vigente.
- Deben definirse y documentarse todos los controles específicos que se realicen y también deben tener en cuenta las responsabilidades que hayan sido asignadas para realizar los controles oportunos que aseguren que se cumplen todos los requisitos de seguridad.
- Es necesario consultar a los asesores legales del Idartes, abogados adecuadamente cualificados, en temas de los requisitos legales específicos que pueden afectar en función de la actividad que realiza cada organización, además de como la información que se crea, en el flujo transfronterizo de datos.
- El tratamiento que se le da a la Seguridad de la Información queda sujeto a los requisitos legales, los reglamentos y las contractuales de seguridad.
- El principal objetivo que se persigue en la seguridad de la información, es evitar los incumplimientos de cualquier obligación legal o contractual.

15.1.2 Derechos de propiedad intelectual (DPI).

Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

- Identificar los requisitos legales, los reglamentarios y los contractuales, además de definir y documentar el enfoque del Idartes.

- Establecer procedimientos para cumplir los Derechos de Protección Intelectual (DPI), se tienen que identificar todos los activos que requieren protección de derechos de propiedad intelectual, bajo las siguientes consideraciones:
- Establecer una política que defina el uso legal del software y los productos de información, estableciendo medidas disciplinarias en caso de infracción.
- Realizar pruebas de la propiedad de licencias, y garantizar que no se excede el número de usuarios permitidos por la aplicación.
- Se tiene que adquirir el software mediante fuentes fiables.

1.5.1.3 Protección de los registros de la organización.

Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.

- Establecer los procedimientos necesarios para cumplir con la Ley Orgánica de Protección de Datos (LOPD)
- Identificar todos los ficheros que contengan datos de carácter personal y establecer el nivel de protección que les corresponda.

15.1.4 Protección de los datos y privacidad de la información personal.

Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.

- Articular acciones para garantizar la seguridad de los datos personales conforme a la Ley de Protección de Datos Personales que reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.
- El Idartes realiza la recolección, recepción, almacenamiento, uso, circulación, supresión, procesamiento, compilación, transferencia o transmisión con entidades públicas o privadas con las que se tiene contratos, acuerdos o convenios para que provean servicios al Idartes.
- El tratamiento específico para cada base de datos personales debe ser definido, autorizado previamente, registrado y comunicado al titular de la información:
    - Gestionar de manera oportuna y clara las solicitudes y consultas realizadas por las partes interesadas del Ministerio, relacionadas con la información general sobre lo misional, funciones, trámites, normatividad vigente, procesos, procedimientos y mecanismos de participación ciudadana.
    - Dar respuestas a consultas, reclamos, solicitud de actualización, rectificación o supresión de datos, y revocatorias de la autorización.
    - Registrar la información de datos personales en las bases de datos del Idartes, con la finalidad de analizar, evaluar y generar datos estadísticos, así como indicadores para la formulación de políticas en el sector cultural.

- Configurar los sistemas y aplicaciones teniendo en cuenta la protección de datos personales conforme a las disposiciones sobre protección de datos, que establecen tipologías de datos según el mayor o menor grado de aceptabilidad de la divulgación:
    - Dato Público: Es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.
    - Dato Semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.
    - Dato Privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.
    - Dato Sensible: Es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación.
- Facilitar el ejercicio de los derechos que la ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales y se reconoce a los titulares, causahabientes, representante y/o apoderado, a favor de otro y a las personas que estén facultadas para representar a los niños, niñas y adolescentes, por tanto para garantizar la seguridad de la información y de los datos personales estarán a disposición los mecanismos para que se puedan ejercer los derechos sobre los datos personales a los cuales realiza tratamiento.

15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico
Asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización.

15.2.1 Cumplimiento con las políticas y normas de seguridad.
Se debe garantizar que en las unidades de gestión y demás áreas se lleven a cabo los lineamientos de seguridad de la información para lograr el cumplimiento con la Política de Seguridad de la Información.

- Gestionar la seguridad y privacidad de la información dando cumplimiento adecuado a la legislación vigente analizando los requisitos legales aplicables a la información de derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional.
- Velara por la protección de los registros ante cualquier perdida, destrucción, falsificación acceso o liberación no autorizada de acuerdo con los requisitos legislativos, de reglamentación y contractuales del Idartes.

15.2.2 Verificación del cumplimiento técnico.
Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.

- Realizar de manera periódica revisiones para comprobar el correcto funcionamiento de la Política de Seguridad de la Información en cuanto a los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información.

- Asegurar que todos los lineamientos de seguridad dentro de las áreas de gestión se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad
- En caso de incumplimiento de las acciones de la Política de Seguridad de la Información, se evaluarán y propondrán acciones correctivas
- La Oficina Asesora de Planeación y Tecnologías de la Información debe realizar revisiones mínimo una vez al año del cumplimiento de la Política de Seguridad de la Información
- Es un deber de los servidores púbicos contratistas y terceros del Idartes, conocer esta Política y realizar todos los actos conducentes para su cumplimiento, implementación y mantenimiento

16. MONITOREO Y SEGUIMIENTO

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

17. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad referenciado en la norma ISO-27001, es un documento que lista los objetivos y controles que se van a implementar en la Entidad, así como las justificaciones de aquellos controles que no van a ser implementados. Para el caso específico del Instituto Distrital de las Artes - Idartes, este tipo de análisis se hace evaluando el cumplimiento de la norma ISO-7001 en temas relacionados con la gestión de la seguridad de la información que este estándar especifica; y una vez se complete este análisis se realizará la declaración de aplicabilidad de estos.