Código			Política	
PSI_LAAD_v.1			Políticas de Seguridad de la Información	
Fecha de emisión				
20	11	2020		

Elaborado por:	Revisado por:	Aprobado por:
Yezid Ospina Piñeros – ETB Christian Giovanni López Hormiga - ETB	Juan Carlos Parada – Alta Consejería Distrital TIC María del Pilar Niño _ Alta Consejería Distrital TIC Lina María Cruz Silva – Empresa de Acueducto y Alcantarillado de Bogotá Sandra Patricia Palacios Jiménez – Secretaria Distrital de Planeación	Manuel Riaño – Líder Proyecto para la constitución de La Agencia Analítica de Datos del Distrito

TABLA DE CONTENIDO

1. Generalidades

1.1 Introducción

El manejo de grandes volúmenes de información supone riesgos que se constituyen en retos para quienes tienen la responsabilidad de salvaguardar los datos de la ciudadanía, que son usados con el ánimo de tomar decisiones en procura de su propio bienestar. Conscientes de tal responsabilidad, en La Agencia de Analítica de Datos del Distrito (en adelante la LAAD) tenemos la misión, no sólo de realizar un tratamiento con total transparencia y ética en el manejo de los datos, sino de proteger la información con los más altos estándares de seguridad para el logro de los objetivos y la tranquilidad de nuestros grupos de interés.

Con lo anterior y teniendo en cuenta que LAAD tiene a su cargo la integración, articulación, centralización del almacenamiento de datos y analítica de estos entre los sectores de la administración distrital, las empresas privadas y la ciudadanía, se hace necesario establecer unos lineamientos concretos, claros y medibles para lograr proteger, preservar y gestionar tal información frente a la posibilidad de materialización de riesgos de seguridad.

Esta política de seguridad de la información junto con la política de tratamiento de datos personales, conforman el conjunto de directrices necesarias para la protección de la información que es gestionada en LAAD.

1.2 Objetivo del documento

Establecer los criterios y lineamientos que deben aplicarse para todos los procesos, tecnología y personas frente a la información gestionada por LAAD, para su eficaz uso, con el fin de establecer y mantener un ambiente controlado de riesgos internos o externos, deliberados o accidentales, relativos a la seguridad de la información, particularmente frente a la confidencialidad, integridad, disponibilidad, trazabilidad, accesibilidad, legalidad, confiabilidad y no repudio de la información.

1.3 Alcance del documento

Este documento contiene las políticas de seguridad de la información específicas que estipulan la implementación de controles de seguridad de la información en atención a la declaración de aplicabilidad - SOA (por sus siglas en inglés) de LAAD. Está dirigido a trabajadores, terceros (proveedores y contratistas), aliados y asociados involucrados en la generación, almacenamiento, procesamiento, uso, transmisión y eliminación de la información que gestiona LAAD. Por tal motivo el incumplimiento de las políticas aquí expresadas, constituyen en sí mismo un incidente de seguridad de la información, sujeto de los análisis del caso que podrían derivar en acciones tales como las sanciones disciplinarias y/o contractuales pertinentes de acuerdo con la magnitud y características de la situación ocurrida.

1.4 Marco normativo y legal

Esta política se construye, en general, bajo la referencia del estándar internacional de la familia de normas ISO27000 y en particular en lo señalado en la norma ISO/IEC 27001 vigente y su anexo A.

A continuación, se describen los principales componentes de la normatividad de rango constitucional, legal y reglamentaria sobre la seguridad de la información, sin que ello implique que sean los únicos:

a. Artículo 15 de la Constitución Política de Colombia: Derecho fundamental a la intimidad, buen nombre y habeas data.

b. Ley 679 de 2001 “Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución”.

c. Decreto 1524 de 2002 “Por el cual reglamenta el artículo 5o. de la Ley 679 de 2001”.

d. Ley Estatutaria 1266 de 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”.

e. Ley 1273 de 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”.

f. Ley 1336 de 2009 “Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes”.

g. Decreto 235 de 2010 “Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas”.

h. Decreto 2952 de 2010 “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.

i. Ley Estatutaria 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.

j. Decreto Reglamentario 1377 de 2013 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012”.

k. Ley 1712 de 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”.

l. Decreto 886 de 2014 “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos”.

m. Decreto Único 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

n. Decreto 103 de 2015 “Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”.

o. Decreto Distrital 806 de 2019 “Por el cual se reglamenta la implementación, apropiación, adopción, fomento y sostenibilidad del Teletrabajo en organismos y entidades Distritales”.

1.5 Compromiso de LADD frente a la seguridad de la información

LAAD define y establece la política de seguridad de la información con el fin de declarar las responsabilidades y conductas que deben ser observados por cada uno de los miembros responsables de la protección y uso de la información, sus empleados, colaboradores, usuarios de información, de recursos y servicios informáticos; proteger la información de los procesos organizacionales para la prestación de sus servicios; precisando las medidas y controles en búsqueda del buen uso de la información y la disminución en los niveles de exposición al riesgo para el cumplimiento legal y regulatorio nacional y distrital.

LAAD gestiona la integridad, disponibilidad, confidencialidad, trazabilidad, accesibilidad, legalidad, confiabilidad y no repudio de la información requerida de la información, sus procesos relacionados, los sistemas informáticos y el personal involucrado en su operación, manipulación y protección, debido a que son activos esenciales e imprescindibles para el desarrollo del objeto de LAAD misma y de la protección de la privacidad a que tiene derecho la ciudadanía en general. En ese sentido da prioridad a la protección de los activos de la información relacionados con la validación, recolección, integración, almacenamiento, depuración, estandarización, tratamiento, procesamiento, enriquecimiento, visualización y analítica multifinalitaria de datos estructurados y no estructurados.

Todos los trabajadores, contratistas y proveedores son responsables del cumplimiento de las políticas y procedimientos de seguridad establecidos en LAAD y de postular riesgos, ejecutar controles y de reportar incidentes de seguridad de la información sobre los activos de información que les sean pertinentes de acuerdo con su responsabilidad.

Las acciones señaladas deben ser continuamente mantenidas y mejoradas sobre la base metodológica de la norma ISO 27001 vigente, aplicable bajo los lineamientos de gestión que se impartan en LAAD, y los acuerdos interinstitucionales e interempresariales pactados por LAAD en línea con las disposiciones vigentes respecto a delitos informáticos, bancos de datos, bases de datos, datos personales y demás obligaciones legales y regulatorias aplicables.

1.6 Objetivos de seguridad de la información

Con el fin de asegurar la debida protección de la información en las actividades de LAAD, que permita tomar decisiones de política pública, la comercialización de los servicios de analítica, la promoción de la formación de capital humano en analítica de datos, la gestión de alianzas nacionales e internacionales para el intercambio de datos autorizados, metodologías, tecnologías e, inclusive, la posibilidad de apoyar proyectos de ciencia, tecnología e innovación en materia de analítica de datos, se establecen los siguientes objetivos de seguridad de la información los cuales constituyen el horizonte de cumplimiento de LAAD:

a. Cumplir los requisitos legales, regulatorios y contractuales de LAAD frente al manejo seguro de la información.

b. Gestionar los riesgos e incidentes de seguridad de la información.

c. Implementar y evaluar continuamente la eficacia de los controles de seguridad requeridos para cumplir con estas políticas de seguridad de la información.

d. Monitorear y mejorar continuamente las políticas, procedimientos y controles internos que permitan mejorar la seguridad de la información.

e. Formar y sensibilizar periódicamente a los trabajadores y proveedores en el cumplimiento de las presentes políticas y los objetivos aquí establecidos.

1.7 Principios de seguridad y privacidad de la información de LAAD

a. **Protección**: Se crean condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano.

b. **Máxima publicidad**: Las acciones que se ejecuten con la información de los ciudadanos son públicas y transparentes

c. **Ética**: las finalidades para las cuales se usa la información de los ciudadanos guardan en todo momento los preceptos de la ética la moral y las buenas costumbres.

d. **Tratamiento de datos personales**: Corresponde a los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia acceso y circulación restringida, seguridad y confidencialidad establecidos en la ley 1581 de 2012.

1.8 Roles de seguridad de la información

a. **Comité de seguridad y privacidad de la información**: Supervisa y promueve el cumplimiento de las políticas de seguridad y privacidad de la información establecidos garantizando el cumplimiento a la regulación. Adicionalmente evalúa y monitorea los indicadores de cumplimiento de los estándares de seguridad y privacidad establecidos.

b. **Chief Data Officer**: Proporciona la dirección general y la supervisión de la estrategia, arquitectura, gobierno e implementación de casos de uso.

c. **Chief Information Security Officer**: Vela por el cumplimiento de los controles necesarios para cumplir con las políticas de seguridad de la información establecidas.

d. **Gestor de estrategia & arquitectura de ciberseguridad**: Apoya en la definición de la estrategia y arquitectura de ciberseguridad en LAAD.

e. **Gestor de políticas y lineamientos**: Apoya en la definición de la políticas y lineamientos de ciberseguridad en LAAD.

f. **Gestor de riesgo y BCP**: Apoya en la definición de matriz de riesgos y en el plan de continuidad de negocio de la LAAD.

g. **Propietarios de activos de información**: Roles que están al frente de los procedimientos clave en LAAD y que tienen la misión de asegurar la administración correcta de los activos de información durante todo su ciclo de vida, con el fin de proteger la información crítica de LAAD que se encuentra bajo su cargo. Vela por sus activos de información sean debidamente inventariados y autoriza los accesos a la información a su cargo.

h. **Custodio de los activos de información**: Es quien a nombre del propietario administra los controles de seguridad de la información que requieren los activos bajo su cargo.

i. **Oficial de Protección de Datos Personales**: Persona o área, interna o externa, responsable de velar por la implementación efectiva de las políticas y procedimientos para cumplir las normas, así como la implementación de buenas prácticas de gestión de datos personales en LAAD.

j. **Auditor de seguridad de la información**: Persona o área interna o externa responsable de realizar las revisiones independientes de seguridad de la información con el fin de asegurar la mejora continua de la práctica.

k. **Usuario de activos de información**: Todo trabajador o contratista que requiere acceder, según sea pertinente con ocasión de sus responsabilidades, a los sistemas de información o los lugares donde se almacena y procesa información, de acuerdo con su área de trabajo.

1.9 Glosario de términos

Activos de información: Es la información que es usada en LAAD, la cual debe ser valorada porque con ella se logra el cumplimiento de los objetivos de los procesos y por tal razón debe ser protegida.

BCP: El plan de continuidad del negocio, BCP por sus siglas en inglés, es un documento claro, preciso y detallado que específica cómo deben actuar todas

las personas y áreas de LAAD para responder ante una situación crítica o desastre de modo que el impacto para LAAD sea el menos posible.

Cadena de custodia: Es un protocolo de actuación que ha de seguirse con respecto a una prueba, frente a un incidente de seguridad, durante su período de vida o de validez, desde que ésta se consigue o genera, hasta que se destruye o deja de ser necesaria.

Cifrado: Es el proceso mediante el cual se codifica la información de modo que no resulte fácil de entender para quienes no tienen acceso autorizado a ella.

Código malicioso: También conocido como malware, se refiere a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Confiabilidad: Es la gestión mediante la cual se mantienen los datos veraces, completos, actualizados y no duplicados con el fin de sacar el verdadero valor a la información.

Confidencialidad: Se refiere a la preservación de las restricciones o limitantes que se deben fijar para autorizar el acceso y la divulgación de los activos de información, así como los medios para la protección de la intimidad personal y propiedad de la información.

Control de acceso administrativo (NAC): El sistema NAC impide el acceso a la red de los dispositivos que no reúnen los requisitos, colocándolos en un área en cuarentena o concediéndoles acceso restringido a los recursos informáticos a fin de evitar que los nodos inseguros infecten la red.

Controles de seguridad: Son medidas preventivas y reactivas implementadas en procesos, tecnología, infraestructura física y personas que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de los activos de información.

Declaración de aplicabilidad (SOA): La Declaración de Aplicabilidad (SoA por sus siglas en inglés, Statement of Applicability) de la norma ISO 27001, de Sistemas de Gestión de Seguridad de la Información (SGSI), es un documento formado por la relación completa de los controles de seguridad de la información evaluables, que se indican en el anexo A de la norma. En ella LAAD indica si cada uno de ellos es de aplicación o no, detallando los motivos y su estado de implantación. Aunque el Anexo A es la referencia para la implantación de

medidas de protección de la información, LAAD puede añadir otros controles y objetivos de control si lo considera necesario.

Declaración de conformidad: Es la facultad que la ley le otorgó a la Superintendencia de Industria y Comercio – SIC para pronunciarse en los casos no contemplados como excepción a la regla general dispuesta en la ley 1581 de 2012 en el sentido de que se prohíbe la transferencia internacional de datos personales de cualquier tipo a países que no garanticen un nivel adecuado de protección de estos.

Desarrollo seguro: Es una necesidad en el diseño y desarrollo de software. La idea detrás del diseño y desarrollo seguro de aplicaciones es tener en cuenta la seguridad desde el minuto cero del ciclo de vida del software.

Disponibilidad: Acceso oportuno y confiable del uso de los activos de información autorizados. Se define cuanto tiempo se puede estar sin el activo en funcionamiento antes del cual se comienzan a materializar riesgos financieros y operativos.

Escaneos: Es un análisis, identificación y reporte muy sistemático de las vulnerabilidades en cuestión de seguridad que se tienen en una infraestructura de computo. La intención es proteger en el mejor porcentaje posible la seguridad de la información ante el ataque de un ente externo.

Ética: Además de tener una responsabilidad con el bien común, es un compromiso de LAAD con el respeto permanente para con la ciudadanía, el personal, sus asociados, sus proveedores, sus acreedores y el Estado como representante de la sociedad. Así, la ética contribuye a afianzar la credibilidad y la confiabilidad de toda la sociedad en la LAAD, logrando satisfacer los deseos y atendiendo los derechos de todas sus partes interesadas.

FTPS: El Protocolo seguro de transferencia de archivos es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red, basado en la arquitectura cliente-servidor, con el valor adicional de que encripta tanto la información de autenticación como los datos de archivos que están siendo transferidos. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

Habeas data: Habeas significa tener, y data significa datos. Este es el derecho que poseen todas las personas de conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos y los demás derechos libertades y garantías constitucionales, relacionadas con la recolección, tratamiento y circulación de datos personales.

Incidente de seguridad de la información: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una transgresión a la Política de Seguridad de la Información.

Información crítica: Corresponde a aquellos activos de información que cuentan con una criticidad MEDIA o ALTA en la matriz de identificación y clasificación de activos la cual es explicada en los manuales de seguridad de la información.

Integridad: Se refiere a la protección contra la modificación no autorizada, exactitud o completitud de los activos de información. Los criterios de clasificación aplican dependiendo de lo que causan los datos inexactos, incompletos o modificados sin autorización y la facilidad con que se superan tales consecuencias.

ISO27000: Para efectos del presente documento es un conjunto de normas o estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Legalidad: El Principio de Legalidad es un principio fundamental, conforme al cual toda actividad debe realizarse acorde a la ley vigente y su jurisdicción, no a la voluntad de las personas.

Medios extraíbles: Son aquellos soportes de almacenamiento diseñados para ser extraídos de la computadora sin tener que apagarla. Ciertos tipos de medios extraíbles están diseñados para ser leídos por lectoras y unidades también extraíbles.

No repudio: Es un servicio de seguridad que previene que un emisor niegue haber remitido un mensaje cuando realmente lo ha emitido y que un receptor niegue su recepción cuando realmente lo ha recibido.

Riesgos de seguridad de la información: Efecto de la incertidumbre sobre los objetivos se seguridad de la información.

RPO: El Recovery Point Objective es la cantidad de datos que LAAD puede permitirse perder y aun así seguir funcionando si sufre un tiempo de inactividad, es decir, el tiempo máximo aceptable que puede transcurrir entre el momento en que se realizó la última copia de seguridad de los datos. Se refiere al volumen de los datos en el riesgo de pérdida que la LAAD considera tolerable.

RTO: El Recovery Time Objective (RTO) es el tiempo que LAAD necesita para recuperar sus sistemas después de inactividad producida por un desastre, es decir, la cantidad de datos que se pierden y se tienen que volver a ingresar durante el tiempo de inactividad de la red. Describe el intervalo de tiempo que puede pasar antes de que la interrupción comience a impedir las operaciones normales de LAAD.

Transparencia: A través de la transparencia, LAAD hace saber a la sociedad cómo actúa, abriendo paso a posibles críticas o juicios de valor. La vía de la transparencia es la comunicación, por lo que se potencia el sistema comunicativo de la LAAD tanto de manera interna como de manera externa. Todo lo anterior en línea con la ley 1712 de 2014 de transparencia y el derecho de acceso a la información pública nacional.

Trazabilidad: Es la capacidad de conocer todo el ciclo de vida de los datos, desde la fecha y hora exacta en que fue extraído, el momento en que se produjo su transformación, y hasta el instante en que tuvo lugar su carga desde un entorno fuente (servidor, fichero, tabla campo, etc.) a otro de destino.

VPN: Una red privada virtual (VPN por sus siglas en inglés), es una conexión segura y cifrada entre dos redes o entre un usuario determinado y una red. Las VPN permiten navegar por Internet de forma privada.

Vulnerabilidades técnicas: Corresponde a un elemento facilitador que frecuentemente aumenta la probabilidad o el impacto de un riesgo en un sistema de información.

2 Políticas específicas de seguridad de la información

2.1 Gestión de activos de información

2.1.1 Inventario y clasificación

a. Todo activo de información asociado a la información y a las instalaciones de procesamiento debe estar debidamente identificado, caracterizado y clasificados en términos de confidencialidad, integridad, disponibilidad y de acuerdo con los requisitos legales y contractuales. Los activos que no sean información como lo pueden ser centros de procesamiento, deben ser clasificados en términos de la información que allí se almacena.

b. El inventario de activos de información debe ser preciso y permanecer actualizado con una periodicidad mínima de una vez al año. La actualización debe hacerse de acuerdo con los cambios que puedan presentarse respecto a la caracterización y clasificación de los activos a través de su ciclo de vida. El ciclo de vida de la información corresponde a su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción.

c. El inventario de activos de información debe ser coherente y acorde a otros inventarios como por ejemplo las tablas de retención documental o la documentación de soporte a los procesos.

d. El esquema de clasificación de los activos de información debe ser estándar para toda todas las áreas de LAAD de manera que se cuente con un entendimiento común de los requisitos de protección y se pueda aplicar la protección adecuada.

2.1.2 Propiedad y etiquetado

a. Todos los activos de información deben tener un propietario.

b. Se debe asignar la propiedad de los activos cuando estos se crean o cuando se transfieren a LAAD.

c. El propietario del activo debe ser responsable de la administración correcta del activo durante todo su ciclo de vida; garantizar que todos sus activos

hagan parte del inventario; asegurarse de que sus activos se clasifiquen o protejan adecuadamente; debe definir y revisar periódicamente las restricciones de acceso a sus activos; debe asegurarse de un manejo adecuado cuando se eliminen o destruyan sus activos.

d. El propietario del activo debe ser una persona o área con el empoderamiento necesario para tomar decisiones sobre el activo de acuerdo con lo señalado en estas políticas. Él puede delegar las tareas rutinarias, es decir a un custodio que resguarde los activos diariamente, pero la responsabilidad sigue siendo suya. El propietario de los activos está asociado a un rol, de manera que, si un propietario se desvincula de LAAD, quien asuma ese rol asumirá la propiedad de los activos.

e. Se debe implementar un procedimiento para el etiquetado de la información que se encuentra en formato físico o electrónico. El etiquetado de cada activo debe reflejar la manera como es clasificado y debe ser fácilmente identificable salvo en los casos en que el activo haya sido clasificado con una criticidad alta.

f. Los procedimientos de etiquetado de la información deben ser claramente divulgados entre trabajadores y contratistas.

2.1.3 Medios extraíbles

Los medios extraíbles tales como USB, CD, DVD, discos externos, tarjetas de memoria, cintas, etc., pueden contener información crítica desde el punto de vista de la seguridad de la información, por lo tanto y teniendo en cuenta que su etiquetado no debe revelar esa clasificación, se hace necesario algunas pautas para su administración:

a. Se debe contar con autorización para el retiro de las instalaciones de procesamiento o administrativas de LAAD y se debe mantener registro de tales retiros para poder mantener un seguimiento de auditoría.

b. Todos los medios se deberían almacenar en un entorno seguro y protegido, de acuerdo con las especificaciones del fabricante.

c. Se deben utilizar técnicas criptográficas para proteger los datos de los medios extraíbles en caso de que ellos estén clasificados como críticos.

d. Por defecto los puertos a dónde se puedan usar medios extraíbles deben estar deshabilitados, así que el uso de los medios extraíbles debe contar con aprobación y, en ese sentido, se debe monitorear la transferencia de información a estos medios.

e. Se debe almacenar más de una copia de datos valiosos en medios separados para reducir el riesgo accidental de daños o pérdidas de datos.

f. Los medios que contienen información crítica se deben almacenar y eliminar de manera segura, es decir, mediante la destrucción o bien a través de técnicas de borrado seguro de datos para el uso por parte de otra aplicación dentro o fuera de LAAD.

g. La eliminación de los medios con información crítica se debe registrar para mantener un seguimiento de auditoría.

h. Al acumular medios para su eliminación, se debe considerar controles seguros de custodia debido al efecto de agregación, que puede hacer que una gran cantidad de información no crítica se vuelva crítica.

i. En caso de requerir trasportar medios físicos de almacenamiento de información fuera de LAAD, el empaque debe ser suficiente para proteger los contenidos de daños físicos que lleguen a ocurrir durante el tránsito de acuerdo con las especificaciones del fabricante, por ejemplo, protección contra factores ambientales que puede reducir la efectividad de la restauración de los medios, como la exposición al calor, a la humedad y a los campos electromagnéticos. Se deben mantener registros, identificando el contenido de los medios, la protección aplicada, así como también un registro de las veces en que se transfirió a los custodios en tránsito y un recibo en el lugar del destino.

2.1.4 Cifrado de la información

La definición de las reglas relacionadas con el uso de controles criptográficos debe tener en cuenta una evaluación de riesgos previa sobre los activos de información, con el fin de identificar aquellos que podrían ser sujetos a tales controles, la cual ayudará a determinar el nivel de protección que debe recibir la información.

Bajo criterios estratégicos, financieros o de mercado, que tendrán que ser evaluados en las instancias pertinentes, se debe asegurar el uso adecuado y eficaz de cifrado.

2.1.5 Borrado, eliminación y destrucción

Los activos de información y los datos críticos deben estar adecuadamente protegidos por los propietarios o responsables contra su pérdida, destrucción, o falsificación. Todo disco duro el cual contenga información de la organización debe contar con un borrado seguro al momento de hacer una asignación de este activo, en cualquier caso, sujeto a las definiciones establecidas en las tablas de retención documental (TRD) asociadas, cuyo contenido deberá guardar relación directa con la gestión del ciclo de vida de los datos.

2.2 Recursos Humanos

2.2.1 Antes, durante y después de la relación laboral

Antes de la relación:

a. La verificación de los antecedentes de los candidatos a ser trabajadores de LAAD, además de realizarse de acuerdo con las leyes y normativas pertinentes, deberá hacerse proporcional a la clasificación de la información a la que accederán y a los riesgos identificados para las responsabilidades que tendrán. Donde un trabajo, ya sea de empleo inicial o por ascenso, requiera que la persona tenga acceso a las instalaciones de procesamiento de información y, en particular, si se maneja información crítica, se deben considerar más verificaciones y en mayor detalle.

b. Los procedimientos deben definir los criterios para las revisiones de verificación de antecedentes, es decir, quién es idóneo para seleccionar a las personas y cómo, cuándo y por qué se realizan las revisiones de verificación.

c. Se debe garantizar un proceso de selección para los contratistas. En estos casos, el acuerdo entre la organización y el proveedor debe especificar las responsabilidades para realizar la selección teniendo en cuenta la

proporcionalidad señalada respecto a la clasificación de la información a la que accederán y a los riesgos identificados para las responsabilidades que tendrán.

d. Todos los trabajadores y contratistas a los que se les otorga acceso a información crítica deben firmar un acuerdo de confidencialidad y no divulgación antes de darles acceso a las aplicaciones o a las instalaciones de procesamiento de información.

e. Los acuerdos contractuales con trabajadores y contratistas deben incluir las responsabilidades legales en cuanto a leyes de derechos de autor y de protección de datos personales. Adicionalmente deben incluir la obligación del cumplimiento de las políticas de seguridad de la información y de protección de datos personales, tanto de LAAD como de las Entidades que entregan información e inclusive las de los ciudadanos.

f. Los acuerdos contractuales con trabajadores y contratistas deben incluir las medidas que se tomarán si el trabajador o contratista no cumple con los requisitos de seguridad de LAAD. Adicionalmente se debe especificar que la reserva de la información sigue vigente después de la terminación de la relación laboral o contractual con LAAD, hasta los límites que la ley permita.

Durante la relación laboral:

Para los trabajadores y contratistas que tengan relación con LAAD, es necesario que se asegure lo siguiente:

g. Antes de que tengan acceso a la información crítica o a los sistemas de información, deben suministrárseles las instrucciones preliminares sobre sus roles y responsabilidades en cuanto a seguridad de la información.

h. Se debe establecer y ejecutar un plan anual de sensibilización y capacitación sobre el cumplimiento de las presentes políticas y la implementación de controles para proteger la información, conforme a sus roles y responsabilidades en relación con las actividades de LAAD. Lo anterior en línea con el plan institucional de capacitación referido en el decreto 612 de 2018.

i. Se les debe proporcionar un canal de denuncias anónimas para denunciar transgresiones a estas políticas y a los procedimientos de seguridad de la información.

j. Específicamente para los trabajadores de LAAD, debe existir un proceso disciplinario formal y comunicado y siempre vigente para investigar a los trabajadores que presumiblemente han trasgredido estas políticas. El proceso disciplinario debe garantizar un trato justo y correcto para los trabajadores sospechosos de cometer transgresiones a la seguridad de la información. El proceso disciplinario se debe utilizar como elemento disuasivo para evitar que los trabajadores transgredan las políticas y procedimientos de seguridad de la información de LAAD. Los actos deliberados deben requerir acciones inmediatas.

Después del a relación laboral:

k. Ante cambios de cargo o terminación de contrato laboral, el trabajador debe hacer entrega formal de los activos de información que le fueron asignados por LAAD para sus actividades laborales. Esta política deberá regirse por los lineamientos en cuanto a gestión de activos físicos vigente que estén definidos en LAAD.

l. Todos los accesos tanto a sitios físicos como a sistemas de información deben ser eliminados inmediatamente se produzca una desvinculación laboral.

m. La desvinculación de un trabajador o un contratista debe ser divulgada a las áreas con las cuales, con ocasión sus responsabilidades, tiene interacción con el fin de mitigar la posibilidad de que se le llegue a compartir información de LAAD.

n. Al momento de la desvinculación LAAD debe asegurarse de hacer cumplir el clausulado de los acuerdos de confidencialidad que se hayan perfeccionado con trabajadores, contratistas y terceros.

2.2.2 Uso aceptable de activos

Las siguientes son las políticas de uso aceptable aplicables a trabajadores, contratistas y terceros, frente a todos los sistemas en los cuales se genera, procesa, almacena, transmite o elimina información y datos, con ocasión de la actividad de LAAD, las cuales deben ser leídas, aceptadas y firmadas por los usuarios de los sistemas:

a. Todos los sistemas informáticos de LAAD están destinados únicamente a propósitos laborales.

b. Toda la información física o electrónica incluyendo comunicaciones, mensajes y archivos, que se genera, procesa, almacena, transmite o elimina con ocasión de la actividad de LAAD, es propiedad de ésta y como tal está prohibido su uso para propósitos diferentes a los debidamente establecidos en los procesos y lineamientos de LAAD.

c. Está prohibido cualquier uso de los activos de información de LAAD con fines de tipo personal que interfiera en las labores de los trabajadores o contratistas.

d. No se deben utilizar los servicios tecnológicos de LAAD para campañas de recaudación de fondos, para obras benéficas, proselitismo político o religioso, actividades de negocios privados, publicidad, ventas, mercadeo, promociones, apuestas, etc., a título personal, distribución de cadenas de mensajes, propagación de falsas noticias, contenido Sexual / Pornográfico, Racismo / odio, cadenas (chistes, oraciones, etc.) que puedan generar discriminación, mensajes difamatorios, calumniosos, amenazantes o lesivos a los intereses de LAAD, de otros trabajadores, contratistas o de otras personas o instituciones, cualquiera que sea su naturaleza, así como para el envío de archivos no autorizados y que puedan ser considerados como fuente de virus, entre otros archivos con extensiones .pif, .scr, .exe, .com, .bat.

e. Está prohibida la creación y el intercambio de información cuyo contenido sea ofensivo, acosador, despectivo, difamatorio, obsceno, amenazador o que contenga lenguaje soez, así como cursar información que vaya en contravía de los valores y objetivos de LAAD.

f. No se deben utilizar los servicios tecnológicos de LAAD para ejecutar prácticas ilegales o en general métodos de comunicación no autorizados en los términos legales y regulatorios.

g. De acuerdo con lo dispuesto en la Ley 679 de 2001 y el Decreto 1524 de 2002, y sus respectivas modificaciones, normatividad que expresamente prohíbe el alojamiento de contenidos de pornografía infantil, los usuarios de las licencias de los servicios informáticos de LAAD deberán abstenerse de: (i) Alojar en la nube imágenes, textos, documentos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con menores de edad. (ii) Alojar en la nube material pornográfico, en especial en modo de imágenes o videos, cuando existan indicios de que las personas fotografiadas

o filmadas son menores de edad. (iii) Alojar en la nube vínculos o "links", sobre sitios telemáticos que contengan o distribuyan material pornográfico relativo a menores de edad. Adicionalmente, y sin perjuicio de la obligación de denuncia consagrada en la ley para todos los residentes en Colombia, los administradores y usuarios de los servicios informáticos de LAAD deberán denunciar ante las autoridades competentes cualquier acto criminal contra menores de edad de que tengan conocimiento, incluso de la difusión de material pornográfico asociado a menores. (v) Abstenerse de usar las licencias de los servicios informáticos de LAAD para divulgación de material ilegal con menores de edad. El incumplimiento de las obligaciones y prohibiciones mencionadas puede acarrear al usuario, además de las sanciones penales a que haya lugar, la imposición por parte del Ministerio de Tecnologías de la Información y las Comunicaciones de multas previstas en las normas vigentes aplicables.

h. No se debe comercializar con terceras personas los servicios de LAAD.

i. Está prohibida la difusión y descarga de material discriminatorio, difamatorio, acosador, ofensivo, pornográfico u obsceno.

j. No se deben utilizar los servicios informáticos de LAAD para el acceso y uso de material y contenidos ilícitos que violen la propiedad intelectual, las normas sobre derechos de autor (marcas registradas, patentes, secretos industriales o comerciales, música, video, fotos e imágenes) cuyas consecuencias se prevé en las leyes sobre la materia.

k. Ningún dato personal debe quedar expuesto en Internet.

l. Toda transacción ejecutada sobre los sistemas de información de LAAD, podrá ser sujeta a monitoreo y seguimiento.

m. En atención a esta política de uso aceptable, cualquier uso inadecuado de los sistemas que contienen información de LAAD, será objeto de las investigaciones pertinentes de manera que podrá llegarse a las acciones disciplinarias correspondientes o hacer efectivas las cláusulas sancionatorias a que haya lugar.

2.2.3 Devolución de activos

a. Los activos de información físicos y electrónicos previamente entregados en propiedad o encomendados por LAAD a trabajadores, contristas y terceros, deben ser devueltos como requisito a la formalización de la finalización de la relación laboral o contractual.

b. Si surge la situación en la cual el trabajador, contratista o tercero use de manera autorizada un equipo de su propiedad, se deben seguir procedimientos formales para garantizar que la información pertinente se transfiera a LAAD y que se elimine de manera segura del equipo.

c. En los casos donde el trabajador, contratista o tercero cuenta con conocimiento importante para las operaciones continuas, dicha información se debe documentar y transferir a LAAD.

d. Durante el período de aviso de despido, LAAD debe controlar las copias no autorizadas de la información pertinente (es decir, propiedad intelectual) de los trabajadores y contratistas desvinculados.

2.2.4 Escritorio y pantalla despejada

a. La información física y los medios extraíbles con activos de información críticos o con datos críticos de LAAD, entre los que se incluyen los datos personales que sean tratados, debe guardarse bajo llave (gabinete, archivador u otro medio físico seguro) cuando no está en uso, especialmente ante ausencias temporales o prolongadas y según el riesgo catalogado para el activo de información.

b. Deben tomarse medidas para el bloqueo automático de pantallas luego de un tiempo de inactividad. No obstante, siempre que un trabajador, contratista o tercero se ausente de su lugar de trabajo, debe bloquear su estación de trabajo, computador de escritorio o portátil de manera que se proteja el acceso a sistemas, aplicaciones, servicios y en general cualquier información de LAAD.

c. Deben tomarse las precauciones necesarias para que ningún tipo de información escrita quede desatendida en ventanas, vidrios y tableros, para lo cual será necesario que al ausentarse de salas de reuniones o lugares de trabajo en general, la eventual información escrita, sea eliminada.

d. Deben tomarse las medidas necesarias para que no esté disponible para su uso, papel reusable con datos críticos, entre los que se incluyen los datos personales que trata LAAD.

e. No se deben tener accesos directos a activos de información críticos en el computador asignado, con el fin de evitar daño, hurto, modificación, eliminación o accesos no autorizados.

2.2.5 Transferencia de información

a. La información electrónica crítica comunicada en forma de elemento adjunto, debe enviarse usando técnicas criptográficas.

b. No deben usarse las cuentas de correo personales públicas y/o gratuitas como Yahoo, Hotmail, Outlook, Gmail, ni redes sociales públicas como Whatsapp o Facebook. Queda prohibido el reenvío automático de correos electrónicos a este tipo de cuentas.

c. No se deben dejar mensajes que contienen información crítica en máquinas contestadoras o buzones de chat, debido a que personas no autorizadas pueden volver a reproducir los mensajes, se podrían almacenar en sistemas grupales o almacenar incorrectamente como consecuencia de una mala manipulación.

Los contratos de transferencia de información deben incorporar lo siguiente:

d. Procedimientos para garantizar la capacidad de seguimiento y no repudiación.

e. Responsabilidades en caso de incidentes de seguridad de la información, como la pérdida de datos.

f. Mantener una cadena de custodia para la información durante el tránsito.

g. Normas técnicas mínimas para la transmisión y para registrar y leer la información y software.

h. Responsabilidades para controlar y notificar la transmisión, el despacho y la recepción.

i. En caso de trasporte físico, acuerdos de garantía en depósito y normas de identificación de Courier.

j. No debe revelarse información crítica de LAAD en conversaciones a las cuales puedan tener acceso personas no autorizadas como lo pueden ser ascensores o lugares públicos.

2.2.6 Dispositivos móviles

La utilización de dispositivos móviles tales como celulares, laptops, tabletas, etc., que contengan información de LAAD, debe ser segura de manera que no se vea comprometida esta información. Para tal efecto se deben tener en cuenta los siguientes lineamientos:

a. No se debe dar acceso a dispositivos móviles a la red sin que pasen las medidas de control de acceso (NAC).

b. Todos estos dispositivos móviles deben ser debidamente registrados para control y seguimiento, por ejemplo, para su entrada y salida de las instalaciones.

c. Deben definirse controles de versión de software para la instalación de parches y restricciones de software y conexión a sistemas de acuerdo con su uso.

d. Deben contar con protección contra malware.

e. Deben contar con respaldo.

f. Se deben guardar todas las precauciones al utilizar dispositivos móviles en lugares públicos, salas de reuniones y otras áreas sin protección.

g. Se debe contar con protección para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos dispositivos, es decir, mediante el uso de técnicas criptográficas o mediante la obligación del uso de información de autenticación secreta.

h. Se debe establecer un procedimiento específico que considere los requisitos legales, de seguros y otros de seguridad para casos de robo o pérdida de dispositivos móviles.

i. Los dispositivos que contengan información crítica no se deben dejar sin supervisión y, donde sea posible, se deben guardar con llave o se deben utilizar bloqueos especiales para proteger a los dispositivos.

j. Si surge la posibilidad de uso de dispositivos móviles de uso privado para el manejo de la información de LAAD, se debe separar el uso privado del uso corporativo, incluyendo el uso de software para apoyar dicha separación y proteger los datos de LAAD en un dispositivo privado.

2.2.7 Teletrabajo

Si surge la necesidad de ejecutar actividades de manejo de información desde locaciones remotas fuera de las instalaciones de LAAD, sea porque operativamente genera valor o porque se realice con ocasión de algún tipo de contingencia, se deben tener en cuenta los siguientes lineamientos, teniendo en cuenta en todo caso lo señalado en el decreto Distrital 806 de 2019 frente a implementación, apropiación, adopción, fomento y sostenibilidad del Teletrabajo en organismos y entidades Distritales:

a. Cuando sea necesario transmitir información magnética o electrónica valorada como crítica, deberá hacerse por un medio seguro alterno, preferiblemente cifrado como VPN o FTPS. En caso de no ser posible porque no se tenga habilitada esta opción con el destinatario, los archivos a ser transmitidos deberán estar protegidos contra lectura y con el envío de claves de protección por un canal diferente.

b. En el desarrollo de actividades de trabajo remoto es responsabilidad de trabajadores, contratistas y terceros la de velar porque sus familiares y visitantes no hagan uso de los equipos corporativos de LAAD ni del acceso por cualquier medio a la red ni a sistemas de la organización.

c. Cuando en el desarrollo de actividades de trabajo remoto sea requerido el uso de WIFI domésticos, los trabajadores, contratistas y terceros deben seguir las siguientes recomendaciones de seguridad: Cambiar la configuración predeterminada del enrutador y cambiar la contraseña del WIFI a una segura en atención a las recomendaciones de la política de

responsabilidades de los usuarios frente a la información de autenticación secreta, establecida en este documento.

d. En el desarrollo de actividades de trabajo remoto, no deben usarse servicios de alojamiento de archivos públicos o personales como nubes públicas, ni correos públicos o personales como Yahoo, Hotmail o Gmail. Únicamente deben utilizarse los canales oficiales ofrecidos por LAAD.

e. Se debe contar con una alternativa tecnológica segura de comunicación y trabajo colaborativo instalado en el equipo, para las personas que ejecutan actividades en trabajo remoto y estas personas deben dar prelación al uso de dicha alternativa.

f. Se debe contar con el debido soporte tecnológico a través de los canales pertinentes para los usuarios que ejecutan actividades en trabajo remoto.

g. Se deben establecer definiciones del trabajo permitido, las horas de trabajo, la clasificación de información que se puede tener y los sistemas y servicios internos que se autoriza al teletrabajador a acceder

h. Se deben definir procedimientos sobre auditoría y monitoreo de seguridad sobre las actividades de teletrabajo.

2.2.8 Seguridad en la gestión de proyectos

Se debe integrar la seguridad de la información en la administración de proyectos de LAAD sin importar el tipo de proyecto. De acuerdo con lo anterior se establecen los siguientes lineamientos:

a. Se deben incluir los objetivos de seguridad en los objetivos de cada proyecto.

b. Se debe realizar una evaluación de riesgos de seguridad de la información en una etapa temprana del proyecto para identificar los controles necesarios a implementar.

c. La seguridad de la información debe ser parte de todas las fases de la metodología de gestión de proyectos que se use en LAAD.

d. Se debe abordar y revisar las implicaciones de seguridad de la información de manera regular en todos los proyectos.

e. Se deben definir y asignar las responsabilidades para la seguridad de la información a los roles establecidos en los métodos de administración del proyecto.

2.3 Control de acceso

a. Los controles de acceso a los activos de información deben tener un propietario designado, quien tiene la responsabilidad de garantizar que se clasifican adecuadamente, revisar las restricciones de acceso y la seguridad del activo.

b. Estos controles son tanto lógicos para los sistemas de información, como físicos para los lugares donde se encuentra información física o digital alojada.

c. La fortaleza de los controles de acceso debe corresponder con la clasificación de la información a la que se accederá. En consecuencia, se debe contemplar la clasificación de los activos de información al momento de definir los controles requeridos para su protección en cuanto a la posibilidad de accederlos, tal y como se establece en el manual de seguridad de información.

d. Los usuarios no deben tener la posibilidad de autorizarse a sí mismos los acceso físicos y lógicos a dónde se almacena la información. Estas autorizaciones deben realizarse bajo los procedimientos de gestión de acceso que deben establecerse en LAAD.

2.3.1 Administración de acceso a los usuarios

a. Para usar sistemas de información o plataformas de servicios se debe contar con la autorización del propietario de la información que se pretende gestionar.

b. Los privilegios de los usuarios deben ser autorizados por el propietario de la información que los usuarios bajo su cargo pretenden gestionar, con base a su necesidad específica de uso y a los requisitos mínimos para sus roles o funciones.

c. Al proporcionar derechos de acceso a un determinado usuario, los propietarios de la información asociada a los sistemas deben verificar que el nivel de acceso otorgado es adecuado para las políticas de acceso del presente documento.

d. Se debe asegurar que los derechos de acceso no estén activados sin que finalice el flujo gestión de acceso.

e. LAAD debe mantener un registro centralizado de los derechos de acceso otorgados a los diferentes usuarios para acceder a los sistemas de información y plataformas de servicios.

f. Se debe identificar los usuarios con acceso privilegiado asociados con cada aplicación y sistema o plataforma.

2.3.2 Administración de contraseñas

Se deben seguir los procedimientos establecidos para la gestión de contraseñas, velando siempre por mantener los accesos mínimos requeridos.

Cada miembro de LAAD y demás personas a quienes se asignen permisos para el acceso a la información debe mantener confidenciales e intransferibles sus credenciales de acceso. Se debe solicitar a los usuarios firmar una declaración donde indique que mantendrán la información de autenticación secreta de manera personal.

a. Se deben establecer mecanismos para verificar la identidad de un usuario antes de proporcionarle información de autenticación secreta nueva, reemplazo o temporal.

b. No se debe proporcionar información de autenticación secreta por ningún medio escrito sin cifrar.

c. Los propietarios de los activos que gestionan los usuarios bajo su cargo deben revisar de manera periódica, los derechos de acceso de esos usuarios y después de cada cambio de rol, traslado o desvinculación con LAAD. La revisión se debería realizar a intervalos más frecuentes si los derechos de acceso son privilegiados.

d. Debe conservarse la trazabilidad de ajustes o cambios en los roles asignados a los usuarios.

e. Cuando se requiera un nivel alto de autenticación y verificación de identidad, lo cual sucede cuando la clasificación de la información es de confidencialidad reservada, los propietarios de los activos de información deben gestionar la utilización de métodos alternativos a las contraseñas, como medios criptográficos, tarjetas inteligentes, tokens, o medios biométricos. Estos métodos deberán estar preestablecidos en un portafolio de soluciones viables por el área de tecnología encargada de tal suministro.

2.3.3 Responsabilidades de los usuarios frente al uso o manejo de la autenticación

Las actividades de usuarios operadores y administradores en los sistemas de procesamiento de información o sus componentes, están condicionadas a monitoreo. El acceso a esta información debe ser usada para los fines permitidos por la ley.

a. Los usuarios deben manejar sus credenciales de autenticación de forma secreta y garantizando que no se divulgue.

b. Las contraseñas o cualquier otro método de autenticación son de uso personal e intransferible.

c. Ninguna contraseña debe ser expuesta a terceros por medio de stikers, en papel, en archivos de software o en algún otro medio que se les parezca. No deben usar las ayudas de los navegadores de internet donde guardan sus credenciales.

d. El cambio de contraseña debe contar con las recomendaciones definidas como seguras que deberán socializarse. Se deben implementar controles tecnológicos que aseguren unas limitaciones mínimas que mitiguen el riesgo de que personas no autorizadas consigan conocer, por medios automatizados o no, las contraseñas de acceso. Las limitaciones para aplicar deben ser:

   • Estar compuesto por lo menos de 12 caracteres

   • Un carácter no debe ser usado secuencialmente más de 2 veces.

   • La contraseña se debe cambiar por lo menos cada 30 días

   • La contraseña debe incluir por lo menos 2 caracteres numéricos y 2 caracteres alfabéticos.

   • Contener caracteres alternados en mayúsculas y minúsculas.

   • No se podrá reutilizar hasta 5 contraseñas ya empleadas anteriormente

2.3.4 Control de acceso de los sistemas de información

a. El sistema no debe mostrar ningún tipo de identificador o mensaje de ayuda al usuario hasta que finalice la respectiva autenticación

b. Al momento de hacer la validación de los datos de autenticación el sistema no debe indicar qué parte de los datos son correctos o incorrectos.

c. Estos sistemas deben guardar la información del usuario cuando su ingreso es exitoso o fallido, con la fecha correspondiente.

d. La contraseña ingresada en el sistema debe estar ofuscada u oculta.

e. Debe contar con un temporizador el cual cierre la sesión cuando se detecte inactividad en la sesión.

f. El uso de las contraseñas debe cumplir los criterios anteriormente mencionados.

g. En caso de cuentas administrativas, es necesario el uso de un sistema de control de acceso a las contraseñas administrativas, garantizando la generación de una nueva contraseña cada vez que se pide dicho acceso.

2.4 Seguridad física y del entorno

2.4.1 Áreas seguras

a. Cuando se definan perímetros de seguridad física, se deben considerar los requisitos de seguridad de los activos de información dentro del perímetro y los resultados de una evaluación de riesgos de seguridad de la información.

b. No deben existir brechas en el perímetro o en las áreas donde se almacena o procesa información crítica. El techo exterior, las paredes y el piso del sitio deben ser de construcción sólida y todas las puertas externas deben estar protegidas adecuadamente contra el acceso no autorizado con mecanismos de control físico; las puertas y ventanas se deben cerrar con llave correctamente, cuando se dejan sin vigilancia y se deben considerar una protección externa para las ventanas, en particular a nivel del suelo.

c. Se debe contar con un área de recepción atendida por una persona u otros medios para controlar el acceso físico al sitio o al edificio; el acceso a los sitios y al edificio se deben restringir solo al personal autorizado.

d. Las puertas contra incendios en un perímetro de seguridad deben tener alarma, ser monitoreadas y probadas en conjunto con las paredes para establecer el nivel de resistencia necesario de acuerdo con las normas aplicables.

e. Las instalaciones de procesamiento de información que administra LAAD deben estar separadas físicamente de las que administran los proveedores.

f. Se debe prestar especial atención a la seguridad del acceso físico en el caso de los edificios que albergan activos para diferentes organizaciones entre las que se llegue a encontrar LAAD.

Respecto a los controles de acceso a las áreas dónde se almacena o procesa información, se tiene:

g. Se debe registrar la fecha y la hora de entrada y salida de las visitas y, se debe supervisar a todas las visitas a menos que su acceso haya sido aprobado anteriormente; solo se les debe otorgar acceso para propósitos específicos y autorizados y se debe emitir de acuerdo con las instrucciones de los requisitos de seguridad del área y a los procedimientos de emergencia. Se debe autenticar la identidad de las visitas con un medio adecuado.

h. El acceso a las áreas donde se procesa o almacena la información crítica se debe restringir a las personas autorizadas solo mediante la implementación de controles de acceso adecuados, es decir, al implementar un mecanismo de autenticación de dos factores o biometría en caso de información crítica.

i. Se debe mantener y monitorear de manera segura un libro de registro físico o una auditoría de seguimiento electrónica de todo el acceso.

j. Todos los trabajadores y contratistas deben portar algún tipo de identificación visible y se deben notificar inmediatamente al personal de seguridad si encuentran visitas sin compañía de alguien de LAAD y a cualquier persona que no porte una identificación visible.

k. Los derechos de acceso físico a las áreas protegidas se deben revisar y actualizar de manera regular y, revocar cuando sea necesario.

Respecto a las actividades en áreas dónde se almacena o procesa información crítica, se tiene:

l. Las áreas dónde se almacena o proceso información crítica deben estar ubicadas de tal manera que se evite el acceso del público en general.

m. No se deben permitir los equipos fotográficos, de video o audio, como las cámaras de dispositivos móviles, a menos que se autoricen.

2.4.2 Equipos seguros

a. Los equipos, la información o el software no se deben retirar de las instalaciones sin una autorización previa.

b. El uso de cualquier tipo de equipos de almacenamiento y procesamiento de información fuera de las dependencias de LAAD debe ser debidamente autorizado. Esto se aplica a los equipos de propiedad de LAAD y a los equipos de propiedad privada que se utilizan a nombre de LAAD.

c. Los equipos y medios que se sacan de las dependencias no se deben dejar sin supervisión en lugares públicos.

d. Se deben verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos críticos y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.

2.5 Seguridad de las operaciones

2.5.1 Gestión del cambio

Todo cambio que tenga o pueda tener algún tipo de influencia sobre los sistemas de información o la infraestructura tecnológica que lo soporta, debe ser sometido a análisis y aprobación por un proceso formal de control de cambio.

2.5.2 Gestión de capacidad

Para cada sistema de información de LAAD, el área de Tecnología deberá determinar regularmente el nivel de utilización de sus recursos, así como la respectiva demanda. Esta información permitirá establecer proyecciones sobre la capacidad de los recursos del sistema.

2.5.3 Controles criptográficos

a. LAAD debe asegurar el uso adecuado y eficaz de cifrado para proteger la confidencialidad, la autenticidad y/o la integridad de los activos que se consideren importantes. Esto sin importar donde sean guardados estos activos.

b. Para la gestión de claves de cifrado, se deben desarrollar e implementar controles para el uso, protección y gestión del ciclo de vida de dichas claves de cifrado.

c. Deben plantear controles en los canales utilizados para la transmisión de esta información.

2.5.4 Separación de ambientes de desarrollo, pruebas y operación

a. Todo sistema en producción debe tener por lo menos un ambiente de desarrollo que permita probar cualquier cambio y reducir el riesgo de acceso no autorizado.

b. Deben existir mecanismos que garanticen el control de acceso a los ambientes de desarrollo, pruebas y producción.

c. Se debe generar un procedimiento sobre el uso de versiones en el desarrollo y mantenimiento de prácticas de desarrollo seguro.

2.5.5 Protección contra códigos maliciosos

a. Se debe contar con mecanismos de detección de código malicioso en la infraestructura tecnológica de LAAD.

b. Se debe realizar campañas de divulgación con el objetivo de informar a los usuarios acerca de medios de prevención y protección ante software malicioso.

2.5.6 Copias de respaldo

a. Toda información de LAAD debe ser respaldada por copias de respaldo tomadas de acuerdo con los requerimientos aplicables, tanto legales como organizacionales.

b. Estos tiempos deben estar alineados con el RPO y RTO de cada sistema de información, de acuerdo con el análisis de impacto. Así mismo, los registros de copias de respaldo deben ser guardados en una base de datos creada para tal fin.

c. Esta información debe contar con acciones de restauración que garanticen la integridad de la información en casos de emergencia y según sea requerido y autorizado por el propietario del activo de la información. Estas copias deben ser probadas de forma periódica, mínimo una vez al año y deben quedar las respectivas evidencias a la restauración, adicionalmente deben probarse que los archivos de respaldo encriptados pueden ser desencriptados al momento de la restauración.

2.5.7 Registro de eventos y generación de evidencias

a. LAAD debe establecer mecanismos para detectar de manera proactiva, es decir mediante monitoreo continuo, actividades no autorizadas en los sistemas de información, como la activación de los registros de auditoría (logs).

b. Los repositorios o almacenamientos donde se guarden los registros deberán estar protegidos contra accesos no autorizados y/o alteraciones. Las actividades de usuarios operadores y administradores en los sistemas de

procesamiento de información o sus componentes, están condicionadas a monitoreo.

c. Debe acordarse una fuente segura para la sincronización de todos los relojes de sistemas que controlen accesos o generen registros de auditoría.

2.5.8 Integridad del software productivo

Todo software que se ejecute en los equipos de cómputo de LAAD debe originarse de fuentes confiables, para evitar alteraciones no autorizadas. El área correspondiente a el manejo de la tecnología es responsable de verificar las fuentes del software antes de proceder con la instalación. Es necesario realizar almacenamiento seguro de esas fuentes confiables, antes de proceder a instalar el código.

Deben contar con los procedimientos donde se hace referencia al ciclo de vida del desarrollo de software y se indiquen los lineamientos respecto a la integridad del software generado, separación de ambientes y el uso de los datos con respecto a las pruebas generadas.

2.5.9 Gestión de vulnerabilidades técnicas

Se deberá mantener una constante y oportuna revisión de las vulnerabilidades técnicas que son detectadas por la comunidad de seguridad de la información que tengan relación con el software utilizado por LAAD. Se debe evaluar y se deben tomar las medidas necesarias para abordar el riesgo asociado. De acuerdo con lo anterior, las siguientes son las acciones que se deben ejecutar por parte del área responsable:

a. Se deben establecer roles y responsabilidades asociados a la administración de vulnerabilidades técnicas.

b. Se deben definir procedimientos específicos para escaneos planeados o por demanda cuando sean aplicables según el caso.

c. Los escaneos planeados deben efectuarse sobre todos los sistemas de información prioritarios de acuerdo con un plan estructurado por cada área, siempre y cuando cada sistema prioritario se escanee al menos cuatro (4) veces al año.

d. Las vulnerabilidades identificadas deberán ser priorizadas para su tratamiento de acuerdo con el nivel de riesgo predefinido en los sistemas que se están escaneando.

e. Como mínimo se deben tratar las vulnerabilidades de los activos críticos.

f. Debe fijarse un plazo máximo de tratamiento de las vulnerabilidades de cuatro (4) meses.

g. Debe considerarse si las acciones para remediar las vulnerabilidades son viables frente al riesgo de su implementación.

2.5.10 Mantenimiento de sistemas

a. Todo sistema de información nuevo o cualquier modificación sobre uno existente debe incluir la identificación de requerimientos de seguridad en conjunto con los requerimientos funcionales.

b. Todo componente nuevo o que forme parte de un cambio en un sistema de información debe pasar previamente por un proceso de pruebas que certifique su correcta operación antes de ser puesto en marcha. Los datos de prueba deben ser protegidos de acuerdo con su sensibilidad, para evitar accesos no autorizados y fugas de información.

c. Los sistemas de procesamiento y almacenamiento de información de los sistemas operativos y aplicaciones deben contar con la última versión más estable emitida por el fabricante, con el fin de dar el aseguramiento adecuado. Si estos no pueden ser actualizados esta excepción deberá ser documentada y un plan de gestión de riesgos implementado.

d. Se debe contemplar en el mantenimiento y en la fase de los desarrollos, el establecimiento de buenas prácticas que provean el diseño, aseguramiento y ejecución para la protección de la información.

2.6 Seguridad en las comunicaciones

2.6.1 Seguridad de las redes

a. Toda conexión hacia las redes de LAAD, que provenga o pase a través de redes inseguras o desconocidas deberá contar con mecanismos de protección (ej. autenticación, cifrado y manejo de la integridad), de acuerdo con los riesgos identificados.

b. Todas las redes de LAAD deben contar con mecanismos de segregación acordes a la sensibilidad de la información. Deben establecerse medidas que restrinjan el acceso a puertos remotos de diagnóstico o configuración, con una autorización apropiada.

2.6.2 Correo electrónico

a. El uso del correo electrónico, servicio de mensajería Web y demás recursos que comprende (calendario, gestión de tareas, entre otros), es proporcionado para fines establecidos por LAAD, como los laborales para el caso de trabajadores y terceros. Todo trabajador, contratista, etc., entiende y acepta que la cuenta que se le asigna es personal e intransferible y se compromete a salvaguardar la contraseña asignada, a cambiarla con frecuencia o cada vez que sea solicitado y a no compartirla con otros usuarios.

b. LAAD se reserva el derecho de proveer este servicio directamente o mediante un proveedor, de establecer la ubicación física de la información y de hacer los cambios que considere pertinentes.

2.6.3 Uso de internet y de la red interna

a. LAAD provee acceso a Internet para los diferentes miembros con el objetivo de facilitar el logro de la misión. En consecuencia, todos los usuarios deben acogerse a los lineamientos de esta política.

b. LAAD se reserva el derecho de restringir el acceso a sitios que puedan afectar la productividad, la seguridad de su información o su personal.

c. Los usuarios deberán abstenerse de visitar sitios restringidos por LAAD de manera directa o indirecta.

d. Así mismo, toda actividad relacionada con navegación en Internet puede ser registrada, LAAD podrá revelar cualquier acceso cuando una autoridad judicial así lo requiera.

e. Según sus funciones de trabajo, será asignado su rol de navegación. Todo tipo de conexiones hacia otras redes, ya sean privadas o públicas, deben ser aprobadas previamente por el área de seguridad correspondiente.

2.7 Adquisición y desarrollo de sistemas

a. El software utilizado puede ser adquirido a través de terceras partes bajo licencia o desarrollados por personal propio o por un tercero.

b. Todo sistema de información nuevo o cualquier modificación sobre uno existente debe incluir la identificación de requerimientos de seguridad en conjunto con los requerimientos funcionales y pasando por el respectivo proceso de cambios.

c. Todo componente nuevo o que forme parte de un cambio en un sistema de información debe pasar previamente por un proceso de pruebas que certifique su correcta operación antes de ser puesto en marcha.

d. Los datos de prueba deben ser anonimizados y protegidos de acuerdo con su sensibilidad, para evitar accesos no autorizados y fugas de información.

2.8 Proveedores

2.8.1 Relación con proveedores

a. Se deben identificar y documentar los tipos de proveedores, es decir, infraestructura TI, servicios de nube, de conectividad, de georreferenciación, de data, financieros, administrativos, etc., y a quienes y con qué privilegios autorizará a LAAD para acceder a la información.

b. Se debe definir un proceso y ciclo de vida estandarizado para administrar las relaciones con los proveedores.

c. Se deben establecer procedimientos para monitorear la adherencia a los requisitos de seguridad de información establecidos para cada tipo de proveedor y tipo de acceso.

d. Se deben establecer controles de precisión y nivel de detalles para garantizar la integridad de la información o el procesamiento de información que entregan las partes de los acuerdos.

e. Deben definirse programas de capacitación y concienciación para el personal de LAAD que interactúa con el personal de proveedores, sobre el compromiso y el comportamiento con base al tipo de proveedor y el nivel de acceso del proveedor a la información de LAAD.

f. Se debe establecer cuáles son los tipos de obligaciones legales, regulatorias y contractuales que les son aplicables a los proveedores en materia de protección de la información y velar por su cumplimiento.

g. Cualquier movimiento, cambio o transición que involucre activos de información en la operación de los proveedores, debe administrarse de manera que se conserven los controles y requisitos de seguridad de la información establecidos.

2.8.2 Acuerdos contractuales

a. En los contratos con los proveedores se debe contemplar el cumplimiento de esta política en lo que es pertinente al objeto contractual, además de la

obligación del proveedor de realizar los acuerdos necesarios con sus propios proveedores, para cumplir con lo pertinente.

b. Los contratos deben garantizar que el proveedor maneje la información que LAAD le confía con los más altos estándares de confidencialidad, integridad y disponibilidad.

c. Se garantice contractualmente el aislamiento de la información de LAAD respecto de la información de otros clientes que tenga el proveedor.

d. Obligación del proveedor de informar oportunamente a LAAD sobre la ocurrencia de incidentes de seguridad de la información y de la colaboración durante su remediación.

e. Obligación del proveedor de establecer las contingencias necesarias para continuar con la gestión de información que LAAD le ha confiado.

f. Siempre que el tratamiento de los datos se realice fuera del territorio colombiano, el contrato de servicios de computación en la nube debe adecuarse a lo establecido en el numeral 2.2.2.25.5.2 del Capítulo 25, Sección 5, del Decreto Único 1074 de 2015, de manera que el control y responsabilidad en el tratamiento de datos esté siempre en cabeza de LAAD como responsable. Si por alguna razón el contrato no logra ajustarse a los términos señalados en el Decreto Único 1074 de 2015, se deberá solicitar la declaración de conformidad pertinente a la Superintendencia de Industria y Comercio.

g. En los acuerdos interinstitucionales de suministro de información debe quedar claro que toda información personal suministrada debe contar con la autorización del tratamiento de datos personales por parte del titular con las finalidades establecidas en la Política de Tratamiento de Datos Personales de LAAD.

h. Debe conocerse la cadena de subcontratación, exigirse que se proteja en todo momento la confidencialidad, integridad y disponibilidad de la información en esta cadena y que se revelen expresamente las zonas geográficas dónde se alojaran los datos confiados por LAAD.

i. En los contratos con los proveedores se debe establecer la obligación del proveedor de colaborar con la gestión de los riesgos de seguridad de la información de acuerdo con los lineamientos de identificación y clasificación de activos de la información y de gestión de riesgos de LAAD y por tanto la

obligación de cumplir con las reglas de uso aceptable de la información, incluido el uso inaceptable, en caso de ser necesario.

j. Implementar controles para que el personal contratado tenga los estudios de seguridad pertinentes a la clasificación de la información a acceder.

k. En los contratos con los proveedores se debe establecer la obligación del proveedor de cumplir con los requisitos legales y normativos, incluida la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.

l. Debe incluirse el derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo.

2.8.3 Monitoreo y revisión de los servicios contratados

a. La responsabilidad de administrar las relaciones del proveedor se debe asignar a una persona o equipo de administración de contratos.

b. Se deben monitorear los niveles de desempeño del servicio con el fin de verificar la adherencia a los acuerdos.

c. Se deben revisar los informes de servicio producidos por el proveedor y organizar reuniones de avance de manera regular según lo requieren los acuerdos.

d. Se deben realizar auditorías de seguridad de la información a los proveedores y efectuar un seguimiento de los problemas identificados.

e. Se debe proporcionar información sobre los incidentes de seguridad y revisar esta información según sea necesario conforme a los acuerdos.

f. Se debe revisar los aspectos de seguridad de la información de las relaciones que tiene el proveedor con sus propios proveedores.

g. Se debe asegurar que el proveedor mantiene una capacidad de servicio suficiente junto con planes de trabajo diseñados para garantizar que se

mantienen los niveles de continuidad en el servicio luego de grandes fallas o desastres en el servicio.

h. Revisar que los cambios en los acuerdos contractuales en el servicio del proveedor realizados de manera unilateral o bilateral garanticen la continuidad de la adherencia de los requisitos de seguridad.

2.9 Gestión de incidentes de seguridad de la información

2.9.1 Definición de procedimientos

a. Se debe asegurar que el personal competente maneje los problemas relacionados a los incidentes de seguridad de la información dentro de la organización, se implemente un punto de contacto para la detección e informe de los incidentes de seguridad y se mantengan los contactos correspondientes con las autoridades, grupos de interés externos o foros que manejen los problemas relacionados con los incidentes de seguridad de la información.

Se deben establecer procedimientos para:

b. La planificación y preparación de la respuesta ante incidentes.

c. Monitorear, detectar, analizar e informar sobre eventos e incidentes de seguridad.

d. Registrar actividades de administración de incidentes.

e. Administrar y guardar evidencia forense.

f. La evaluación y la decisión sobre los eventos de seguridad de la información y la evaluación de las debilidades en la seguridad de la información.

g. La respuesta incluidos aquellos para el escalamiento, la recuperación controlada desde un incidente y la comunicación a las personas internas y externas u organizaciones.

2.9.2 Reporte

a. Los trabajadores y contratistas deben estar en conocimiento de su responsabilidad para informar los eventos de seguridad de la información lo más pronto posible, del procedimiento para informar eventos de seguridad de la información y el punto de contacto al que se debería informar los eventos.

Las situaciones que se deben informar como eventos de seguridad son:

b. Control de seguridad ineficaz

c. Incumplimiento de la integridad, la confidencialidad o las expectativas de disponibilidad de la información.

d. Errores humanos.

e. Incumplimiento de esta política o la de tratamiento de datos personales.

f. Incumplimientos en las disposiciones de seguridad física.

g. Cambios no controlados en los Sistemas de Información.

h. Fallas en el software o hardware.

i. Transgresiones de acceso.

Adicionalmente se debe requerir a los trabajadores y contratistas que utilizan los sistemas y servicios de información de LAAD, anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios.

2.9.3 Evidencia y evaluación

a. Se deben evaluar los eventos de seguridad de la información y se deben decidir si se clasificarán como incidentes de seguridad de la información. La clasificación y la priorización de incidentes debe ayudar a identificar el impacto y el alcance de un incidente.

b. Se deben definir y aplicar procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia con el objetivo de lograr una eficiente respuesta al incidente y para propósitos de acciones legales y disciplinarias.

c. Las acciones para la identificación, recopilación, adquisición y preservación de evidencia deben considerar: la cadena de custodia, seguridad de la evidencia, seguridad del personal, roles y responsabilidades del personal involucrado, competencia del personal, documentación y una sesión informativa.

d. Se deben registrar los resultados de la evaluación y la decisión en detalle con fines de referencia y verificación futuros.

2.9.4 Respuesta y aprendizaje

a. Se debe recopilar la evidencia tan pronto como sea identificado el incidente, con el objetivo de gestionarlo, es decir, reanudar el nivel de seguridad normal y luego iniciar la recuperación necesaria.

b. Se deben ejecutar los escalamientos necesarios en atención al alcance de solución de acuerdo con los roles definidos.

c. Todas las actividades de respuesta se deben registrar correctamente para el posterior análisis.

d. Se debe comunicar la existencia del incidente de seguridad de la información o cualquier detalle relacionado a los grupos de interés pertinentes.

e. Se deben gestionar las debilidades de la seguridad de la información que causan o contribuyen al incidente.

f. Una vez que se ha gestionado el incidente correctamente, se debe cerrar y registrar formalmente.

g. Se debe realizar un análisis post - incidente, según sea necesario, para identificar el origen del incidente y así implementar medidas para que no vuelva a suceder.

h. Se debe utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información, haciendo énfasis en aquellos recurrentes o de alto impacto, para reducir la probabilidad o el impacto de incidentes futuros. La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de contar con controles mejorados o adicionales para limitar la frecuencia, el daño y el costo de las ocurrencias futuras o bien se deben considerar en el proceso de revisión de la presente política.

2.10 Seguridad en la continuidad del negocio

a. En comparación con las condiciones operacionales normales, los controles de seguridad de la información deben mantenerse a pesar de que LAAD deba operar en contingencia ante situaciones adversas, es decir durante una crisis o desastre.

b. Se debe realizar un análisis de impacto para los aspectos de seguridad de la información, con el fin de determinar los requisitos de seguridad de la información que se aplican a situaciones adversas en las cuales no sea viable mantener los controles que se tienen en situación normal.

c. Debe existir una estructura de administración adecuada para preparar, mitigar y responder ante un desastre que utiliza personal con la autoridad, la experiencia y la competencia necesaria.

d. Se debe definir personal de respuesta ante crisis o desastres con la responsabilidad, la autoridad y la competencia necesaria para administrar un incidente de esta naturaleza y mantener la seguridad de la información.

e. Deben desarrollarse y aprobarse planes documentados, procedimientos de respuesta y recuperación detallando cómo LAAD administrará un desastre y mantendrá la seguridad de su información a un nivel predeterminado.

f. Se debe verificar mínimo dos (2) veces al año la valides y eficacia de los controles de seguridad de la información establecidos e implementados para situaciones de crisis o desastre.

g. Se deben identificar los requisitos para la disponibilidad de los sistemas dónde se almacena y procesa información de LAAD. Cuando no se pueda garantizar la disponibilidad a través de la arquitectura de sistemas existente, se deben considerar los componentes o arquitecturas redundantes y

probarlas para garantizar que la conmutación por error de un componente a otro funcione adecuadamente.

2.11 Cumplimiento

Todos los requisitos estatutarios, normativos, regulatorios, contractuales y legales y el enfoque de la organización para cumplir con estos requisitos se deben identificar, documentar y mantener al día de manera explícita para LAAD y para cada sistema dónde se almacene o procese información. Por lo mismo deben considerarse estos requisitos de manera explícita en los acuerdos que se establezcan con terceros dónde se involucren sistemas de información.

2.11.1 Seguridad de las bases de datos personales

a. El acceso a la información personal sensible, es decir aquella cuyo uso inadecuado puede generar discriminación, debe hacerse únicamente por el personal que trata esa información con ocasión exclusiva de la finalidad para la cual se tiene recolectada y con la debida autorización del titular, salvo en los casos que por ley no sea requerida dicha autorización. Los controles de acceso a esta información, tanto a nivel tecnológico como físico, deben tener especial seguimiento.

b. Deben existir controles para que sólo personal debidamente autorizado, tenga acceso a copiar o transferir masivamente información de datos personales

c. Las bases de datos personales no deben estar almacenadas en computadores personales, ellos deben reposar en los sistemas informáticos o de almacenamiento propios o contratados y con los privilegios de acceso debidamente gestionados y justificados. En caso de que se tenga información personal en medios de almacenamiento extraíble debe atenderse lo definido en la política de seguridad pertinente a estos medios.

d. Los trabajadores, contratistas y terceros deben mantener la información personal íntegra cada vez que sea tratada por ellos. Los dueños de los activos deben velar porque la gestión de sus procesos apoye sistemáticamente esta misión.

e. Se entiende que los controles de seguridad de la información que se implementan a partir de los lineamientos establecidos en las políticas de este documento aplican para los activos de información entre los que se encuentran las bases de datos de información personal.

f. Deben ejecutarse auditorias periódicas que permitan identificar oportunidades de mejora en el tratamiento de datos personales que contribuyan a su protección eficaz y al cumplimiento de la ley particularmente a lo establecido en el régimen de protección de datos personales.

g. Queda prohibido el uso de las bases de datos personales de los proveedores, contratistas o terceros para fines comerciales a menos que se haya obtenido autorización previa, expresa e informada sobre esta finalidad, por parte de ellos.

h. Siendo posible compartir información personal, sea porque los titulares de la información dieron autorización, o sea porque medie una razón legal, judicial o contractual, sólo se pueden circular al interior y fuera de LAAD aquellos datos que sean estrictamente necesarios para los fines de su uso.

2.11.2 Derechos de autor y propiedad intelectual

Los derechos de propiedad intelectual incluyen los derechos de autor del software o documentos, derechos de diseño, marcas registradas, patentes y licencias de código de fuente, por lo tanto, se deben tener en cuenta las siguientes consideraciones:

a. La marca, avisos, nombres comerciales, propaganda comercial, dibujos, diseños, logotipos, textos, etc. deben hacerse a partir de los lineamientos gráficos y de diagramación definidos y deben ser de exclusiva propiedad de LAAD, a menos que de manera previa y expresa se autorice a terceros para su uso. De acuerdo con lo anterior se deben proteger de conformidad con lo establecido por las normas nacionales e internacionales de protección de la Propiedad Industrial y del Derecho de Autor.

b. Sólo se debe adquirir software a través de fuentes conocidas y de confiable reputación, para garantizar que no se transgreda el derecho de autor.

c. Se deben mantener registros de activos adecuados y la identificación de todos los activos con los requisitos para proteger los derechos de propiedad intelectual.

d. Se deben mantener pruebas y evidencias de la propiedad de las licencias, discos maestros, manuales, etc.

e. Se deben implementar controles para garantizar que cualquier número máximo de usuarios permitidos dentro la licencia no se exceda.

f. Se deben realizar revisiones periódicas para verificar que solo se instale software y productos licenciados y que se mantengan las condiciones adecuadas de las licencias.

g. Las adquisiciones de software deben estar avaladas por el área responsable de Tecnología y por el líder pertinente en LAAD.

h. Se deben cumplir con los términos y condiciones para el software y la información obtenida de redes públicas.

i. No se deben duplicar, convertir a otro formato ni extraer grabaciones comerciales (película, audio) a no ser que lo permita la ley de derecho de autor.

j. No está permitido copiar libros, artículos, informes u otros documentos en su totalidad o en parte, que no sean los permitidos por la ley de derecho de autor.

2.11.3 Auditorías de seguridad de la información

a. Los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información y el tratamiento de datos personales se deben revisar independientemente en intervalos planificados y como mínimo una vez al año o cuando ocurren cambios significativos en la operación de LAAD.

b. La auditoría la deben realizar personas independientes del área bajo revisión, es decir, la función de auditoría interna, un gerente independiente o una organización externa que se especialice en dichas revisiones. Las personas que realizan estas revisiones deben contar con las habilidades y experiencia adecuada.

c. Los resultados de la revisión independiente se deben registrar e informar al más alto nivel de LAAD.

d. Se deben mantener registros de la auditoría y se deben emprender los análisis de causa pertinentes y la generación de acciones para responder a los hallazgos, incluidos fechas y responsables.

e. Adicional a las auditorías independientes, los líderes de área deben identificar y verificar que se cumplen los requisitos de seguridad de la información definidos en estas políticas y procedimientos pertinentes. Se debe considerar el uso de informes para la revisión regular eficiente.

f. Los sistemas dónde se almacena y procesa información se deben revisar regularmente para verificar su cumplimiento con estas políticas y los procedimientos pertinentes.

g. Las revisiones de cumplimiento técnico involucran el análisis de los sistemas operacionales para asegurarse que se han implementado correctamente los controles de hardware y software. Este tipo de revisión de cumplimiento requiere la experiencia técnica de un especialista. También abarcan, por ejemplo, las pruebas de penetración y las evaluaciones de vulnerabilidad. Esto puede ser útil para detectar las vulnerabilidades en el sistema y para inspeccionar cuan eficaces son los controles para evitar el acceso no autorizado debido a estas vulnerabilidades.

Control de Cambios:

Versión	Descripción del Cambio	Fecha del Cambio
1.0	Documento inicial	20/11/2020