Políticas de Seguridad de la Información

Versión	Fecha	Elaborado por	Revisado por	Aprobado por
2.0	Agosto de 2022	Julio César Cárdenas Galindo Camilo Andrés Díaz Trillos Juan David Rey Conrado	Equipo Directivo de Ágata	Asamblea de accionistas

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. Consciente de tal responsabilidad, la Agencia de Analítica de Datos S.A.S. – ÁGATA tiene 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 sus grupos de interés.

Con lo anterior y teniendo en cuenta que ÁGATA tiene a su cargo la integración, articulación y analítica de los datos 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, gestionar y divulgar tal información con el fin de realizar el tratamiento adecuado de los riesgos de seguridad de la información.

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 ÁGATA. Derivados de ellas, existen una serie de manuales de seguridad de la información y privacidad que documentan lineamientos particulares, procedimientos establecidos y otras medidas. Dichos manuales son compartidos y socializados con las partes interesadas, con el fin de promover la cultura de seguridad de la información dentro y fuera de la Agencia.

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 ÁGATA, 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, autenticidad 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 ÁGATA. 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 ÁGATA. Por tal motivo, el incumplimiento de las políticas aquí expresadas constituyen en sí mismo un evento 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. Las directrices y lineamientos de este documento son de obligatorio cumplimiento.

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 versión 2013.

A continuación, se describe el marco legal aplicable, 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 1074 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.",

n. 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".

o. Decreto 103 de 2015 "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".

p. 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. Glosario de términos

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (equipos, sistemas, soportes, edificios, personas, entre otras) que tenga valor para la organización.[1]

BCP: El plan de continuidad del negocio, BCP por sus siglas en inglés, está orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.[2]

Cadena de custodia: Proceso continuo y documentado aplicado a los EMP (Elementos Materiales Probatorios) y EF (Evidencia Física), por parte de los servidores públicos y particulares que con ocasión a sus funciones deban garantizar su autenticidad y capacidad demostrativa, mientras que la autoridad competente ordena su disposición final.[3]

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

[1] Modelo de Seguridad y Privacidad de la Información. MinTIC.
[2] ISO/IEC 27000
[3] Manual del Sistema de Cadena de Custodia. Fiscalía General de la Nación.

Código malicioso: También conocido como malware o software malicioso. Se refiere a cualquier tipo de software que realiza acciones dañinas o permite accesos no autorizados en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.[4]

Control: Medida por la que se modifica el riesgo.[5]

Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. [6]

Los términos salvaguarda o contramedida son utilizados frecuentemente como sinónimos de control.

Declaración de aplicabilidad (SOA): La Declaración de Aplicabilidad (SoA por sus siglas en inglés, Statement of Applicability) es un documento que enumera los controles aplicados por el SGSI (Sistema de Gestión de Seguridad de la Información) de la organización, tras el resultado de los procesos de evaluación y tratamiento de riesgos, y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.[7]

Aunque el Anexo A es la referencia para la implantación de medidas de protección de la información, ÁGATA puede añadir otros controles y objetivos de control si lo considera necesario.

[4] ISO/IEC 27000
[5] ISO/IEC 27000
[6] ISO Guide 73:2009
[7] ISO/IEC 27000

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.[8]

Desarrollo seguro: Conjunto de principios de diseño y buenas prácticas a implantar en el ciclo de vida de desarrollo de software (SDLC), para detectar, prevenir y corregir los defectos de seguridad en el desarrollo y adquisición de aplicaciones, de forma que se obtenga software de confianza y robusto frente a ataques maliciosos, que realice solo las funciones para las que fue diseñado, que esté libre de vulnerabilidades, ya sean intencionalmente diseñadas o accidentalmente insertadas durante su ciclo de vida y se asegure su integridad, disponibilidad y confidencialidad.[9]

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.[10]

Dispositivos móviles: Componentes tecnológicos de hardware y software con capacidades de almacenamiento, procesamiento y transmisión de información que por su tamaño pueden ser transportados fácilmente. Se consideran dispositivos móviles los teléfonos celulares, equipos portátiles y tabletas entre otros.

Escaneo de vulnerabilidades: Es un análisis, identificación y reporte sistemático de las vulnerabilidades en cuestión de seguridad que se tienen en una infraestructura de

[8] Guía Declaración de Conformidad. Superintendencia de Industria y Comercio.
[9] Secure Software Development Life Cycle. OWASP.
[10] ISO/IEC 27000

cómputo. La intención es proteger en el mejor porcentaje posible la seguridad de la información ante el ataque de un ente externo.

Evento de seguridad de la información: Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.[11]

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.

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.[12]

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información[13] o cualquier situación que implique la adulteración, pérdida, consulta, uso o acceso no autorizado a la información personal (datos personales).

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.

[11] ISO/IEC 27000
[12] Artículo 3 Ley 1581 de 2012
[13] ISO/IEC 27000

Integridad: Propiedad de la información relativa a su exactitud y completitud.[14]

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 unidades lectoras y unidades también extraíbles.

No repudio: Capacidad de probar la ocurrencia de un evento o acción reclamada y sus entidades de origen.[15]

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.[16]

[14] ISO/IEC 27000
[15] ISO/IEC 27000
[16] ISO-7498-2

Riesgos de seguridad de la información: Efecto de la incertidumbre sobre los objetivos de seguridad de la información.[17]

El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

RPO: El Recovery Point Objective (RPO) es el punto en el tiempo en el que se deben recuperar los sistemas y los datos después de que haya ocurrido un desastre.[18]

RTO: El Recovery Time Objective (RTO) se refiere al tiempo máximo aceptable que puede transcurrir antes de que la falla de una función comercial afecte gravemente a la Agencia. Este es el tiempo máximo acordado para la reanudación de las funciones críticas de Ágata.[19]

Transparencia: A través de la transparencia, ÁGATA 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 ÁGATA 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: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.[20]

[17] ISO/IEC 27000
[18] BCM Institute - Instituto de Gestión de Continuidad del Negocio
[19] BCM Institute - Instituto de Gestión de Continuidad del Negocio
[20] CESID:1997

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.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.[21]

2. Política de Seguridad de la Información

ÁGATA gestiona la integridad, disponibilidad, confidencialidad, trazabilidad, accesibilidad, legalidad, confiabilidad, autenticidad y no repudio de la información requerida, 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 ÁGATA 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.

2.1. Compromiso de ÁGATA frente a la seguridad de la información

ÁGATA define y establece la política de seguridad de la información con el fin de declarar las responsabilidades y conductas que deben ser observadas 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

[21] ISO/IEC 27000

buen uso de la información y la disminución en los niveles de exposición al riesgo para el cumplimiento legal y regulatorio nacional y distrital.

Todos los trabajadores, contratistas, colaboradores y proveedores son responsables del cumplimiento de las políticas y procedimientos de seguridad establecidos en ÁGATA y de postular riesgos, ejecutar controles y de reportar eventos e 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 en observancia de la norma ISO 27001:2013, aplicable bajo los lineamientos de gestión que se impartan en ÁGATA, y los acuerdos interinstitucionales e interempresariales pactados por ÁGATA 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.

2.2. Objetivos de seguridad de la información

Con el fin de asegurar la debida protección de la información en las actividades de ÁGATA, 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 ÁGATA:

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

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

c. Definir e implementar los controles de seguridad y evaluar continuamente su eficacia para cumplir con estas políticas de seguridad de la información y proteger los activos de información conforme al nivel de riesgo aceptable establecido en la organización.

d. Monitorear y mejorar continuamente las políticas, procedimientos y controles internos que permitan fortalecer 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.

2.3. Principios de seguridad y privacidad de la información de ÁGATA

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.

2.4. Roles de seguridad de la información

A continuación se describen, alfabéticamente, los roles más importantes en la gestión de la seguridad de la información de acuerdo con las descripciones de cargo contenidas en el documento "Entregable 8: modelo de negocio, modelo operativo y de gobierno":

a. **Área de Seguridad de la Información:** Unidad Organizacional liderada por el CISO, y perteneciente a la Gerencia de Analítica y Datos, encargada de liderar la estrategia de seguridad de la información y ciberseguridad de Ágata.[22]

b. **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.

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

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

[22] Entregable 8: modelo de negocio, modelo operativo y de gobierno

establecidas. Apoya en la definición de riesgos de continuidad y en el desarrollo del Plan de Continuidad de Negocio (BCP)[23].

e. **Comité de seguridad y privacidad de la información**: Define y establece las políticas de ciberseguridad para la Agencia. Supervisa y promueve el cumplimiento de las políticas de seguridad y privacidad de la información establecidas garantizando el cumplimiento de la regulación. Adicionalmente evalúa y monitorea los indicadores de cumplimiento de los estándares de seguridad y privacidad establecidos. Analiza constantemente el perfil de riesgo de la Agencia para identificar vulnerabilidades, defensas existentes y áreas de mejora.[24]

f. **Custodio de los activos de información**: Es quien a nombre del propietario administra los activos de información bajo su cargo y responde por los controles de seguridad de la información que requieren. En términos del Gobierno de Datos de Ágata este rol lo desempeñan los Data Custodians.

g. **Gerencia de Tecnología:** Implementa, administra y monitorea las herramientas tecnológicas de apoyo y gestión de seguridad de la información, así como las definidas como controles de seguridad. Implementa todas las plataformas tecnológicas de acuerdo con las políticas de seguridad de la información de este documento o cualquier otro complementario[25].

h. **Gestor de estrategia y arquitectura de ciberseguridad**: Apoya en la definición de la estrategia y arquitectura de ciberseguridad en ÁGATA.

[23] El CISO asume el rol del Gestor de riesgo y BCP hasta que esta posición sea ocupada según el plan de contratación de Ágata.

[24] ENTREGABLE 4: Comités ejecutivos

[25] La Gerencia de Tecnología no es un rol específico.Las responsabilidades descritas en este numeral y cualquier otra asignación del presente documento corresponden a todo el equipo de trabajo de la gerencia que por sus responsabilidades esté facultado para su cumplimiento.

i. **Gestor de políticas y lineamientos**: Apoya en la definición de la políticas y lineamientos de ciberseguridad en ÁGATA.

j. **Propietario de activos de información**: Asegura la administración correcta de los activos de información a su cargo y los niveles de aseguramiento durante todo su ciclo de vida. Vela por que sus activos de información sean debidamente inventariados y autoriza los accesos a la información a su cargo. En términos del Gobierno de Datos de Ágata este rol lo desempeñan los Data Owners.

k. **Oficial de Protección de Datos Personales - OPD**: Vela por la implementación efectiva de las políticas y procedimientos para cumplir las normas aplicables, así como la implementación de buenas prácticas de gestión de datos personales y privacidad en ÁGATA.

l. **Usuario de activos de información**: Toda persona 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.

3. Políticas específicas de seguridad de la información

3.1. Gestión de activos de información

3.1.1. Propiedad, inventario, clasificación y etiquetado

a. El Área de Seguridad de la Información en Ágata debe definir, socializar y velar por el uso de un esquema de clasificación de los activos de información estándar para todas las áreas de ÁGATA de manera que se cuente con un entendimiento

común de los requisitos de protección y se pueda aplicar la protección adecuada a cada activo de información.

b. Todos los activos de información deben tener un propietario, el cual se debe asignar cuando los activos se crean o cuando se transfieren a ÁGATA.

c. 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. La propiedad de los activos está asociada a un rol, de manera que, si un propietario se desvincula de ÁGATA, quien asuma ese rol asumirá la propiedad de los activos.

d. Los propietarios de activos de información pueden delegar las tareas rutinarias asociadas con la gestión y la protección de sus activos a otras personas o áreas, sin embargo, se mantendrá responsable de lo señalado en estas políticas. Las personas o áreas en quienes el propietario delega las actividades mencionadas se denominan custodios de activos de información.

e. Los propietarios de los activos de información son responsables de la administración y uso correctos de sus activos, definiendo y revisando periódicamente las restricciones de acceso a estos y garantizando que las protecciones definidas correspondan con su clasificación.

f. Los propietarios de activos de información y los custodios encargados de la administración o protección de estos activos deben entregar la totalidad de los activos y todas sus copias al momento de su retiro de ÁGATA o cuando estos cambien de propiedad.

g. Los propietarios de los activos de información deben identificar, caracterizar y clasificar todos los activos de información asociados a la información y a las

instalaciones de procesamiento, de acuerdo con el esquema de clasificación según confidencialidad, integridad, disponibilidad y los demás requisitos legales y contractuales definidos. 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, procesa o transmita.

h. Los propietarios de los activos de información deben garantizar que todos sus activos hagan parte del inventario. El inventario de activos de información debe ser preciso y permanecer actualizado 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.

i. Los propietarios de los activos de información deben asegurar el manejo adecuado cuando sus activos de información se eliminen o destruyan, de acuerdo con su clasificación.

j. Los propietarios de los activos de información y los custodios de los activos deben asegurar que el inventario de activos de información interrelaciona cada activo de información con otros activos de información o activos de TI con los que tiene algún tipo de dependencia en busca de facilitar los análisis de riesgos e impacto derivados de dichas relaciones.

k. Los propietarios de los activos de información deben asegurar la coherencia entre el inventario de activos de información y otros inventarios, como por ejemplo las tablas de retención documental o la documentación de soporte a los procesos.

l. El Área de Seguridad de la Información en Ágata debe definir, implementar y velar por el uso de 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.

m. El Área de Seguridad de la Información en Ágata debe divulgar claramente los procedimientos de clasificación y etiquetado de la información entre trabajadores y contratistas.

n. Todo usuario que hace uso de activos de información debe garantizar que dicho uso se realiza de acuerdo con los requerimientos de seguridad definidos para tales activos y en ejercicio de sus funciones laborales o contractuales con Ágata.

3.1.2. Medios extraíbles de almacenamiento

Los medios extraíbles de almacenamiento contienen información que debe ser objeto de análisis y clasificación según lo dispuesto en estas políticas. Se definen las siguientes políticas de administración sobre estos dispositivos de almacenamiento:

a. Los propietarios de los activos de información deben velar por el almacenamiento de los activos en un entorno seguro y protegido, de acuerdo con las especificaciones del fabricante y con los criterios de protección según la clasificación de la información que contienen.

b. Los propietarios de los activos de información deben justificar y autorizar el retiro de sus activos a cargo de las instalaciones administrativas o de procesamiento de ÁGATA y deben mantener un registro actualizado de todos los retiros autorizados con fines de auditoría.

c. Los propietarios de los activos de información y los custodios encargados de la administración o protección de estos activos deben utilizar técnicas criptográficas

para proteger los datos almacenados en medios extraíbles en caso de que ellos estén clasificados como críticos.

d. La Gerencia de Tecnología como encargada de la administración de los equipos de cómputo para el procesamiento, almacenamiento o transferencia de información en Ágata debe garantizar que los puertos en donde se puedan usar medios extraíbles de almacenamiento permanecen deshabilitados a menos de que exista una aprobación autorizada por el área encargada de la Seguridad de la Información, en cuyo caso debe monitorear la transferencia de información a estos medios.

e. Cuando la información almacenada en medios de almacenamiento extraíbles es valiosa o se considera crítica, los propietarios de estos activos de información deben asegurar el almacenamiento de más de una copia de estos datos en medios separados para reducir el riesgo de pérdidas de datos por daños o pérdida de los medios.

f. Los propietarios de los activos de información y los custodios encargados de la administración o protección de estos activos deben garantizar la eliminación segura de los datos almacenados en medios extraíbles mediante la destrucción o a través de técnicas de borrado seguro de datos. Estas actividades y la evidencia generada deben quedar registradas con propósitos de auditoría.

g. Si no es posible realizar eliminación inmediata de medios extraíbles de almacenamiento, los propietarios de los activos de información deben entregar en custodia estos medios a un responsable de su almacenamiento quien 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.

h. En caso de requerir el transporte de medios físicos de almacenamiento de información, los propietarios de estos activos de información y los custodios encargados de la administración o protección de estos activos deben velar porque el empaque y embalaje utilizados sean adecuados para garantizar la protección de los contenidos contra daños físicos derivados de la naturaleza de los medios, por ejemplo, daños por exposición al calor o al frío, a la humedad o a los campos electromagnéticos. Los propietarios de los activos de información deben mantener registros en los que se identifique el contenido de los medios, la protección aplicada y las veces en que se transfirió a los custodios en tránsito con evidencia del recibo en el lugar del destino.

i. En caso de requerir el transporte de medios físicos de almacenamiento de información, los propietarios de estos activos de información y los custodios encargados de la administración o protección de estos activos deben implementar técnicas de cifrado de datos para evitar el acceso a los datos por parte de terceros no autorizados.

3.1.3. Cifrado de la información

a. 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.

b. Teniendo en cuenta la criticidad de los datos, los dueños de la información deben asegurar el uso de métodos de cifrado para proteger dicha información.

c. La Gerencia de Tecnología como responsable de la implementación de los controles criptográficos debe mantener un inventario actualizado de todos los controles y analizar periódicamente cada control para garantizar que su solidez se mantiene en el tiempo.

3.1.4. Borrado, eliminación y destrucción

Los activos de información y los datos críticos deben estar adecuadamente protegidos por los propietarios y custodios contra su pérdida, destrucción, acceso o modificación no autorizados por lo que se establecen los siguientes lineamientos para evitar estos riesgos después de terminar su ciclo de vida.

a. Cuando los activos de información deban ser eliminados de acuerdo con las tablas de retención documental (TRD), los propietarios de estos activos de información y los custodios deben garantizar que la información sea eliminada de manera irrecuperable de los activos que corresponda.

b. Ante cambio, reposición o disposición final de activos críticos, los propietarios y los custodios deben velar porque el área encargada de la administración de equipos de cómputo y medios de almacenamiento realicen un borrado seguro que evite la recuperación parcial y total de la información.

c. La Gerencia de Tecnología debe propender por realizar borrado seguro de todos los activos, incluso si estos no contienen activos de información críticos, previa evaluación de la conveniencia, pertinencia y otras implicaciones antes de la reasignación o disposición final de cada activo.

d. La Gerencia de Tecnología debe garantizar que los procedimientos, herramientas y algoritmos utilizados para realizar borrado seguro sean

considerados robustos y que la información eliminada por estos sea totalmente irrecuperable.

3.1.5. 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 ÁGATA, las cuales deben ser leídas, aceptadas y firmadas por los usuarios de los sistemas:

a. Todos los sistemas informáticos dispuestos por ÁGATA están destinados únicamente a propósitos laborales o contractuales claros y previamente establecidos.

b. La gestión de software y aplicaciones en ÁGATA es una responsabilidad exclusiva de la Gerencia de Tecnología por lo que está prohibido descargar, instalar, desinstalar o hacer uso de cualquier software o programa sin la autorización explícita de los responsables del área.

c. 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 ÁGATA, es propiedad exclusiva de la Agencia y como tal está prohibido su uso para propósitos diferentes a los debidamente establecidos en las funciones laborales, las obligaciones contractuales, los procesos y lineamientos de ÁGATA.

d. Está prohibido cualquier uso de los activos de información y sistemas informáticos de ÁGATA con fines diferentes a los laborales.

e. La información crítica debe mantenerse en los sistemas centralizados de información de Ágata. Está prohibido tener información crítica en equipos de cómputo personal o dispositivos móviles sin la debida autorización del dueño de la información y previo concepto técnico basado en riesgos de ciberseguridad.

f. No se deben utilizar los servicios tecnológicos de ÁGATA 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 ÁGATA, de otros trabajadores, contratistas o de otras personas o instituciones, cualquiera que sea su naturaleza, así como para el envío de archivos no autorizados o que puedan ser considerados como fuente de virus.

g. 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 ÁGATA.

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

i. 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 deberán abstenerse de:

(i) Alojar en la nube o en cualquier recurso dispuesto por ÁGATA imágenes, textos, documentos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con menores de edad.

(ii) Alojar en la nube o en cualquier recurso dispuesto por ÁGATA 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 o en cualquier recurso dispuesto por ÁGATA 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 ÁGATA 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.

(iv) Abstenerse de usar las licencias de los servicios informáticos de ÁGATA 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.

j. No se debe comercializar con terceras personas los servicios de ÁGATA a menos que exista autorización previa por parte del gobierno corporativo de la agencia.

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

l. No se deben utilizar los servicios informáticos de ÁGATA para el acceso y uso de material y contenidos ilícitos que violen la propiedad intelectual, las normas sobre

derechos de autor y propiedad industrial (marcas registradas, patentes, secretos industriales o comerciales, música, video, fotos e imágenes) cuyas consecuencias se prevé en las leyes sobre la materia.

m. Ningún dato personal debe quedar alojado en Internet sin las debidas protecciones definidas para tal fin.

n. Toda transacción ejecutada sobre los sistemas de información de ÁGATA podrá ser sujeta a monitoreo y seguimiento.

o. En atención a esta política de uso aceptable, cualquier uso inadecuado de los sistemas que contienen información de ÁGATA 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.

3.1.6. Devolución de activos

a. Los activos de información físicos y electrónicos previamente entregados en propiedad o encomendados por ÁGATA a trabajadores, contratistas 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 ÁGATA 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 ÁGATA.

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

e. Los supervisores de contratos con terceras partes en los cuales Ágata haya dispuesto de activos de información o activos de TI deben garantizar la recolección y disposición adecuada de estos como requisito esencial para realizar el cierre contractual.

3.1.7. Uso de equipos personales

En ÁGATA es permitido el uso de equipos personales de propiedad de empleados y contratistas bajo los siguientes lineamientos:

a. El almacenamiento de información crítica en equipos personales está prohibido.

b. El uso de equipos personales está autorizado dentro y fuera de las instalaciones de Ágata para aquellos empleados y contratistas que de otro modo no podrían realizar las tareas laborales o contractuales bajo su responsabilidad, siempre que cumplan con los requisitos de seguridad definidos en la presente política o en los documentos que la Gerencia de Tecnología defina para tal fin.

c. La información de ÁGATA, de sus clientes o proveedores que sea entregada a los trabajadores y contratistas para que sea procesada, almacenada o transmitida desde sus equipos personales sigue siendo de propiedad de la agencia y por ende mantiene el derecho a controlar dicha información.

d. La Gerencia de Tecnología debe propender por la utilización de herramientas tecnológicas que permitan la configuración de espacios o perfiles de trabajo en los dispositivos personales. Dichos espacios o perfiles deben permitir la separación del uso personal o privado del uso corporativo, garantizando en este último que el almacenamiento de información sea seguro, y si es posible, que las aplicaciones que accedan a la información corporativa estén controladas a través de listas blancas.

e. Los usuarios propietarios de equipos personales deben mantener instalado, actualizado y activo un software antivirus reconocido, incluso si es una versión gratuita. Ante dudas sobre software antivirus, los empleados o contratistas deben preguntar a la Gerencia de Tecnología quien avalará el uso de diferentes opciones de software antivirus gratuitos.

f. Los usuarios propietarios de equipos personales deben mantenerlos actualizados con las últimas versiones y actualizaciones de sistema operativo y aplicaciones.

g. Los equipos personales deben estar protegidos por contraseñas, códigos de acceso, lectores biométricos o cualquier método de control de acceso que evite el uso público o irrestricto del mismo.

h. El uso de sistemas y aplicaciones de la agencia puede estar supeditada a la utilización de software de acceso remoto seguro por lo que el trabajador o contratista que requiera utilizar su equipo personal debe instalarlo. La

instalación y uso de cualquier software corporativo es una aceptación tácita de las políticas de uso asociadas. Los programas de instalación y las instrucciones de instalación y uso deben ser provistos por la Gerencia de Tecnología.

i. Los usuarios de equipos personales no deben dejarlos desatendidos en ningún momento, dentro o fuera de las instalaciones de Ágata.

j. El uso de equipos personales por parte de otros usuarios es permitido siempre que se garantice que estos usuarios no tienen acceso a ninguna aplicación o información de la Agencia.

k. Los usuarios de equipos personales no pueden utilizar, para crear o modificar información de la Agencia, software que no esté dentro de la lista de software autorizado por Ágata así se encuentre instalado en estos equipos.

l. En los equipos personales el software base y cualquier otro software instalado no deben estar activados ilegalmente, crackeados o liberados, evitando de tal manera que puedan ocasionar riesgos en las plataformas tecnológicas de la Agencia

m. Los empleados o contratistas propietarios de los equipos personales no deben almacenar contraseñas ni otros tipos de credenciales de autenticación en dichos equipos.

n. Los empleados o contratistas deben reportar oportunamente la pérdida o robo de los equipos personales que contengan software o información de Ágata sin importar su clasificación con el propósito de determinar el nivel de riesgo asociado a este incidente.

o. Los empleados o contratistas propietarios de los equipos personales deben reportar cualquier indicio de compromiso del equipo o de los sistemas o información de Ágata a través de este.

3.2. Recursos Humanos

3.2.1. Antes, durante y después de la relación laboral

Antes de la relación:

a. La Gerencia de Asuntos Corporativos debe definir los procedimientos y criterios para realizar verificación de antecedentes de candidatos y trabajadores, por primera vez y sus revisiones periódicas.

b. La Gerencia de Asuntos Corporativos debe realizar verificación de los antecedentes de los candidatos a ser trabajadores de ÁGATA de acuerdo con las leyes y normativas pertinentes y en proporcionalidad a la clasificación de la información a la que tendrán acceso y a los riesgos identificados para las responsabilidades.

c. Se debe garantizar un proceso de selección para contratistas proporcional al que tendrían los trabajadores de Ágata. En estos casos, el acuerdo entre Ágata y el proveedor debe especificar las responsabilidades del proceso de selección y los criterios de clasificación de la información y riesgos identificados para las responsabilidades del cargo en selección.

d. La Gerencia de Asuntos Corporativos debe velar porque todos los trabajadores y contratistas a los que se les otorga acceso a información crítica firmen un acuerdo de confidencialidad y no divulgación antes de darles acceso a las

aplicaciones o a las instalaciones de procesamiento de información. Los acuerdos de confidencialidad deben considerar para su vigencia el periodo de relación contractual o laboral más un periodo prudente después de la terminación de dicha relación, hasta los límites que la ley lo permita.

e. Los acuerdos contractuales con trabajadores y contratistas deben incluir las responsabilidades legales en cuanto a leyes de propiedad intelectual 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 ÁGATA como de las Entidades que entregan información.

f. La Gerencia de Asuntos Corporativos debe incluir en los acuerdos contractuales con trabajadores y contratistas las medidas que se tomarán si el trabajador o contratista no cumple con los requisitos de seguridad de ÁGATA o con los acuerdos de confidencialidad celebrados.

g. La Gerencia de Asuntos Corporativos debe informar oportunamente el ingreso de trabajadores y contratistas para que los recursos y accesos sean aprovisionados de acuerdo con los procedimientos definidos.

Durante la relación laboral:

Para los trabajadores y contratistas que tengan relación laboral o contractual vigente con ÁGATA, es necesario que se asegure lo siguiente:

a. Toda la información que se genere, gestione yo transfiera en virtud de la relación laboral es propiedad de ÁGATA, bajo lo cual la Gerencia de Tecnología tendrá la facultad de acceder, monitorear y recaudar en cualquier momento para funciones de control y supervisión, los equipos de cómputo, celulares o cualquier

otro equipo o hardware entregado al trabajador para el cumplimiento de sus funciones.

b. Antes de que tengan acceso a la información crítica o a los sistemas de información, la Gerencia de Asuntos Corporativos debe suministrarles las instrucciones preliminares sobre sus roles y responsabilidades en cuanto a seguridad de la información.

c. La Gerencia de Asuntos Corporativos 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 ÁGATA. Lo anterior en línea con el plan institucional de capacitación referido en el decreto 612 de 2018.

d. Ágata, a través del área que considere pertinente, debe proporcionar un canal de denuncias anónimas para denunciar transgresiones a estas políticas y a los procedimientos de seguridad de la información.

e. Específicamente para los trabajadores de ÁGATA, la Gerencia de Asuntos Corporativos debe establecer un proceso disciplinario formal y comunicado y siempre vigente para investigar a los trabajadores que presumiblemente han transgredido 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 ÁGATA. Los actos deliberados deben requerir acciones inmediatas.

f. Los trabajadores y contratistas de Ágata deben atender, participar y obtener calificaciones aprobatorias en las actividades enmarcadas dentro del programa de sensibilización en Seguridad de la Información, Ciberseguridad y Privacidad.

g. La Gerencia de Asuntos Corporativos debe informar oportunamente las ausencias temporales de trabajadores para que los recursos y accesos sean inhabilitados durante esos periodos de acuerdo con los procedimientos definidos. La misma responsabilidad aplica para los supervisores de contrato cuando la ausencia temporal corresponda a un contratista de ÁGATA.

Después de la relación laboral:

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

i. La Gerencia de Tecnología debe garantizar que todos los accesos tanto a sitios físicos como a sistemas de información deben ser eliminados inmediatamente cuando se produzca una desvinculación laboral.

j. La Gerencia de Asuntos Corporativos debe divulgar la desvinculación de un trabajador a las áreas con las cuales, con ocasión de sus responsabilidades, él tiene interacción con el fin de mitigar la posibilidad de que se le llegue a comprometer información de ÁGATA. La misma responsabilidad aplica para los supervisores de contrato cuando se produzca la finalización de una relación con un contratista.

k. Al momento de la desvinculación laboral o de la finalización de una relación con un contratista se debe asegurar que se hace cumplir el clausulado de los

acuerdos de confidencialidad que se hayan perfeccionado con trabajadores, contratistas y terceros.

3.2.2. Escritorio y pantalla despejada

a. La información física y los medios extraíbles con activos de información críticos o con datos críticos de ÁGATA, 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. La Gerencia de Tecnología debe tomar medidas para el bloqueo automático de equipos de cómputo 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 ÁGATA.

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 de seguridad necesarias para que el papel reutilizable no contenga datos críticos, entre los que se incluyen los datos personales que trata ÁGATA.

e. Se debe evitar dejar documentos impresos desatendidos en las impresoras y en los escritorios de trabajo.

f. 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.

3.2.3. Transferencia de información

a. La información electrónica comunicada en forma de elemento adjunto y cuya clasificación sea crítica debe enviarse usando técnicas criptográficas.

b. No deben usarse cuentas de correo personales públicas y/o gratuitas como Yahoo!, Hotmail, Outlook, Gmail, ni redes sociales públicas como WhatsApp o Facebook para enviar o recibir información crítica de ÁGATA o sus clientes.

c. El reenvío automático de correos electrónicos de ÁGATA a cuentas de correo públicas o gratuitas está prohibido.

d. 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.

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

Los contratos de transferencia de información deben incorporar lo siguiente:

f. Procedimientos para la entrega y devolución de la información.

g. Procedimientos para garantizar la eliminación irrecuperable de la información una vez cumplida la finalidad del contrato.

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

i. Responsabilidades en caso de incidentes de seguridad de la información.

j. Procedimientos de cadena de custodia para la información durante el tránsito.

k. Normas técnicas mínimas para la transmisión y registro de la información.

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

m. En caso de transporte físico, acuerdos de garantía en depósito y normas de identificación de Courier.

n. En caso de que la información objeto del contrato contenga datos personales, se debe especificar la finalidad y objeto que originan la transferencia, las responsabilidades de tratamiento, custodia y protección y las responsabilidades de las autorizaciones de los titulares. Así mismo, en el contrato se deberá dar cumplimiento a los requisitos establecidos en el artículo 2.2.2.25.5.2. del Decreto 1074 de 2015.

3.2.4. Dispositivos móviles

La utilización de dispositivos móviles que tengan acceso a información de ÁGATA, 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.

b. Todos los dispositivos móviles deben ser debidamente registrados para control y seguimiento, por ejemplo, a la 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. Los dispositivos móviles deben contar con protección contra malware de acuerdo con las políticas de este documento y cualquier otro lineamiento corporativo al respecto.

e. Si hay almacenamiento de información crítica en los dispositivos móviles, se debe garantizar que dicha información esté respaldada y cifrada.

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. El uso de dispositivos móviles de propiedad de trabajadores y contratistas está permitido bajo el estricto cumplimiento de los lineamientos dispuestos en el numeral 3.1.7. Uso de Equipos Personales, del presente documento.

3.2.5. Teletrabajo

Para la ejecución de todas las actividades de manejo de información desde locaciones remotas se deben tener en cuenta los siguientes lineamientos:

a. La transmisión de información y el acceso a los sistemas de información o recursos tecnológicos de ÁGATA debe realizarse únicamente a través de protocolos considerados seguros. El uso de protocolos inseguros en ÁGATA está prohibido a menos que por limitaciones tecnológicas no se puedan reemplazar por otros seguros, en cuyo caso se deberá incluir una capa adicional de protección como el uso de conexiones cifradas o el cifrado y descifrado de los datos en los extremos.

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

c. En el desarrollo de actividades de trabajo remoto únicamente deben utilizarse los sistemas de información y recursos tecnológicos oficiales y autorizados por ÁGATA.

d. ÁGATA dispondrá de herramientas y recursos tecnológicos seguros para que sean utilizados por trabajadores, contratistas y proveedores que lo requieran.

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

f. 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.

g. Se deben definir e implementar procedimientos sobre auditoría y monitoreo de seguridad sobre las actividades de teletrabajo.

3.2.6. Seguridad en la gestión de proyectos

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

a. Las estructuras de gobierno de los proyectos en Ágata deben incluir los objetivos de seguridad en los objetivos de cada proyecto.

b. Los responsables de liderar cada proyecto, en conjunto con el Oficial de Protección de Datos, deben realizar una evaluación de riesgos de seguridad de la

información y protección de datos personales en una etapa temprana del proyecto para identificar los controles necesarios a implementar.

c. Los controles de seguridad de la información y privacidad identificados en los análisis descritos en el literal b del presente numeral, deben ser implementados de manera obligatoria y dejar la evidencia de su ejecución.

d. Los requisitos de seguridad de la información deben ser parte de todas las fases de la metodología de gestión de proyectos que se use en ÁGATA.

e. Se debe abordar y revisar las implicaciones de seguridad de la información de manera regular en todos los proyectos especialmente ante cambios en su alcance, definición o ejecución.

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

3.2.7. Procesos y procedimientos

En ÁGATA la definición de procesos y procedimientos debe cumplir con los siguientes lineamientos:

a. Los procesos y procedimientos de Ágata deben estar documentados, ser socializados y aceptados por los usuarios participantes.

b. Los procesos y procedimientos de Ágata deben tener un dueño funcional que se encargue del monitoreo y supervisión de su ejecución y la resolución de posibles incidencias asociadas. Para esto, en la documentación del proceso

deberán definirse los indicadores que se monitorearán constantemente y los valores esperados.

c. Las actividades más importantes de cada proceso deben soportarse preferiblemente sobre sistemas de información que faciliten su ejecución y garanticen la trazabilidad de las acciones realizadas por cada usuario. Se debe propender por la automatización y soporte de procesos completos.

d. Los procesos y procedimientos de Ágata deben garantizar el cumplimiento del principio de segregación de funciones (SoD) para que las actividades que se consideren críticas involucren a varios usuarios que puedan detectar fallos y que eviten que un único usuario pueda ejecutarlas sin supervisión.

e. Los sistemas de información que soporten procesos y procedimientos deben reflejar en su sistema de control de acceso los permisos que cada usuario debe realizar en respeto del principio de mínimo privilegio.

f. Los procesos y procedimientos de Ágata deben ser trazables y dejar evidencia significativa con propósitos de auditoría.

g. Los procesos y procedimientos de Ágata deben ser sometidos a análisis de riesgos con apoyo del Área de Seguridad de la Información para identificar los riesgos y sus tratamientos que garanticen la seguridad y la privacidad. El análisis de riesgos deberá revisarse y actualizarse al menos cada año.

h. Los procesos y procedimientos deben contemplar escenarios de falla en su ejecución y en las herramientas que los soportan para definir estrategias o flujos alternos de ejecución que permitan mantener la operación de Ágata.

i. Cualquier cambio en los procesos o procedimientos debe verse reflejado en su documentación, ser aprobado mínimo por el nivel jerárquico superior al dueño funcional y por las demás partes interesadas y generar una actualización del análisis de riesgos correspondiente para ajustar las medidas de protección.

j. Las actividades de los procesos y procedimientos de Ágata deben ser asignadas a roles o cargos específicos de la compañía para garantizar su cumplimiento. Se debe garantizar que el conocimiento para la ejecución de cada actividad esté replicado en diferentes personas que puedan garantizar la ejecución a pesar de la ausencia del responsable principal.

3.3. 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 que protege. En consecuencia, los propietarios de los activos de información deben contemplar la clasificación de sus activos 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 accesos físicos y lógicos a donde se almacena la información. Estas autorizaciones deben

realizarse bajo los procedimientos de gestión de acceso que deben establecerse en ÁGATA.

e. Se debe propender porque la autenticación de los usuarios se realice a través de un sistema de autenticación centralizado y con uso de tecnologías de una sola autenticación (SSO: single sign-on). En consecuencia, la Gerencia de Tecnología debe implementar, configurar y mantener una solución de autenticación centralizada con los niveles más altos de seguridad, incluyendo el uso de segundos factores de autenticación.

3.3.1. 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. La Gerencia de Tecnología 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. Al menos una vez cada seis (6) meses la Gerencia de Tecnología debe realizar un procedimiento de certificación de accesos mediante el cual se corrobore que los accesos existentes corresponden a autorizaciones válidas y vigentes. Si se identifican diferencias, se deben tomar las acciones necesarias correspondientes para evitar la repetición o reincidencia.

g. La Gerencia de Tecnología debe contar con herramientas y procedimientos para identificar y monitorear a los usuarios con acceso privilegiado de cada aplicación, sistema o plataforma.

h. La Gerencia de Tecnología debe mantener registros de todos los accesos para efectos de auditoría.

3.3.2. 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 ÁGATA 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. Los propietarios de los sistemas de control de acceso o los encargados de su operación deben establecer mecanismos para verificar la identidad de un usuario antes de proporcionarle información de autenticación secreta nueva, reemplazo o temporal.

b. Siempre que se proporcione información de autenticación secreta por algún medio, esta debe estar debidamente cifrada, de acuerdo con el mecanismo definido..

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 ÁGATA. La revisión se debería realizar a intervalos más frecuentes si los derechos de acceso son privilegiados.

d. Los propietarios de los sistemas de control de acceso o los encargados de su operación deben conservar trazabilidad de solicitudes, aprobaciones e implementaciones 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.

f. Las credenciales de autenticación para servicios de integración y credenciales administrativas únicas deben mantenerse en custodia compartida por dos o más personas que garanticen su uso adecuado. El Área de Seguridad de la Información debe servir de custodio de las partes para garantizar que ante la ausencia de alguna de las partes se puede hacer uso de las credenciales.

3.3.3. 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 divulguen.

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 stickers, en papel, en archivos digitales 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 establecimiento o cambio de contraseñas debe estar alineado con las recomendaciones definidas para mantenerlas seguras. La Gerencia de Tecnología debe 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.

3.3.4. Control de acceso de los sistemas de información

a. Los propietarios de los sistemas de control de acceso deben garantizar que estos no muestran 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. Los sistemas de control de acceso deben guardar trazas de auditoría con la información del usuario, el estado exitoso o fallido, el origen o dirección IP y la fecha y hora correspondientes.

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

e. Las plataformas tecnológicas deben contar con un temporizador que cierre las sesiones cuando se detecte inactividad durante un tiempo preestablecido.

f. El uso de las contraseñas debe cumplir los criterios de seguridad anteriormente definidos y cualquier otro que se defina en los manuales que profundicen cada dominio de control.

g. El acceso de usuarios con cuentas privilegiadas o administrativas debe incluir un segundo factor de autenticación que propenda el uso de claves o códigos de un solo uso (OTP por sus siglas en inglés).

h. Ante ausencias prolongadas de los funcionarios o contratistas, como vacaciones, licencias o incapacidades, se debe restringir el acceso a las plataformas tecnológicas de la Agencia, a menos de que exista una autorización expresa por el jefe inmediato.

3.4. Seguridad física y del entorno

3.4.1. 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 sólo 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 ÁGATA 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 ÁGATA.

Respecto a los controles de acceso a las áreas donde 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 sólo 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 debe notificar inmediatamente al personal de seguridad si encuentran visitas sin compañía de alguien de ÁGATA 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 donde se almacena o procesa información crítica, se tiene:

l. Las áreas donde se almacena o procesa 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.

3.4.2. 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 ÁGATA debe ser debidamente autorizado por la Gerencia de Tecnología. Esto se aplica a los equipos de propiedad de ÁGATA y a los equipos de propiedad privada que se utilizan a nombre de ÁGATA.

c. Los usuarios autorizados para retirar equipos y medios de las instalaciones de Ágata los deben mantener siempre bajo supervisión y control en lugares públicos o privados.

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.

e. La Gerencia de Tecnología es la única área de la Agencia autorizada para gestionar el software y hardware de los equipos de Ágata. El retiro o reemplazo de

piezas y la instalación, modificación o desinstalación de software por usuarios diferentes están prohibidos.

f. La Gerencia de Tecnología debe mantener un listado de software adquirido y autorizado y su licenciamiento.

g. El uso de software libre se permite bajo criterios de utilidad para desempeñar funciones laborales o contractuales y con la autorización del Área de Seguridad de la Información después de un análisis de riesgos sobre su utilización.

3.5. Seguridad de las operaciones

3.5.1. 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. La Gerencia de Tecnología debe definir, documentar, liderar y velar por el cumplimiento del proceso de control de cambios.

3.5.2. Gestión de capacidad

Para cada sistema de información de ÁGATA, la Gerencia de Tecnología deberá determinar regularmente el nivel de utilización de sus recursos, así como la respectiva demanda. Esta información permitirá establecer un plan de capacidad tecnológica.

3.5.3. Controles criptográficos

a. ÁGATA 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. Se deben definir e implementar controles en los canales utilizados para la transmisión de esta información.

d. La Gerencia de Tecnología debe garantizar que las herramientas y algoritmos de cifrado utilizados en Ágata se consideren seguros durante su utilización. Si alguno llega a considerarse débil según la industria, la Gerencia debe plantear las acciones necesarias para su reemplazo en el menor tiempo posible.

e. Cuando sea requerido, el Área de Seguridad de la Información debe fungir como custodio de claves de cifrado con el propósito de garantizar su disponibilidad aún en ausencia de su propietario o custodio principal.

3.5.4. Separación de ambientes de desarrollo, pruebas y operación

a. Todo sistema en producción debe tener por lo menos un ambiente pre-productivo que permita probar cualquier cambio y reducir los riesgos derivados de su implementación, en consecuencia la Gerencia de Tecnología debe considerar su

aprovisionamiento desde el momento en que inicia el proyecto o proceso de adquisición.

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

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

d. Los propietarios de activos de información deben garantizar que los niveles de seguridad de sus activos en pre-producción son equivalentes a los implementados en los ambientes de producción.

e. Se debe propender por el uso de datos ficticios en ambientes pre-productivos. En caso de no ser posible, se debe garantizar la impersonalización, ofuscación o aleatorización de datos productivos antes de ser copiados a los ambientes previos.

3.5.5. Protección contra códigos maliciosos

a. La Gerencia de Tecnología debe implementar mecanismos de detección de código malicioso en la infraestructura tecnológica de ÁGATA.

b. Los mecanismos de detección de código malicioso deben configurarse para que ningún usuario pueda desactivarlos o desinstalarlos por su propia cuenta.

c. Los mecanismos de detección de código malicioso deben gestionarse de manera centralizada y actualizar su base de detección por lo menos una vez al día.

d. Los servicios de colaboración, correo electrónico y cualquier otro que almacene, procese o transmita información en forma de archivos o documentos digitales deben contar con protección contra códigos maliciosos.

e. Los mecanismos de detección de códigos maliciosos deben analizar procesos en ejecución, espacios de almacenamiento y tráfico de red en equipos de cómputo, servidores y otras plataformas.

f. El Área de Seguridad de la Información debe realizar campañas de divulgación con el objetivo de informar a los usuarios acerca de medios de prevención y protección ante software malicioso.

3.5.6. Copias de respaldo

a. Toda información de ÁGATA debe ser respaldada con copias de respaldo tomadas de acuerdo con los requerimientos aplicables, tanto legales como organizacionales. La Gerencia de Tecnología debe definir y comunicar la estrategia de copias de seguridad asociada con cada sistema de información.

b. La frecuencia con que se realizan las copias de respaldo debe estar alineada con los tiempos RPO y RTO definidos para cada sistema de información en los análisis de impacto.

c. Se deben mantener los registros de las copias de respaldo con fines de auditoría.

d. La información crítica debe ser respaldada con copias de seguridad que utilicen técnicas criptográficas para evitar el acceso no autorizado a la información respaldada.

e. Para evitar que las copias de seguridad sean comprometidas por ataques de virus, malware o ransomware se debe propender por el uso de técnicas de una sola escritura y múltiples lecturas (WORM por sus siglas en inglés).

f. Las copias de seguridad deben ser probadas frecuentemente para garantizar la efectividad del proceso de respaldo y la integridad de la información respaldada, prestando especial atención a las copias cifradas.

g. La Gerencia de Tecnología debe definir procedimientos para restaurar las copias de seguridad garantizando la integridad de la información y, según sea requerido, incluir las autorizaciones respectivas por el propietario del activo de la información.

h. El proceso de restauración de copias de seguridad para cada sistema o plataforma debe ser probado al menos una vez al año, dejando las respectivas evidencias con fines de auditoría.

3.5.7. Registro de eventos y generación de evidencias

a. La Gerencia de Tecnología debe garantizar que los registros de auditoría (logs) de todos los sistemas de información y componentes tecnológicos se encuentren activados para tener trazabilidad de todas las acciones realizadas sobre ellos.

b. La Gerencia de Tecnología debe definir procedimientos de monitoreo continuo sobre los registros de auditoría para detectar de manera oportuna actividades no autorizadas sobre los sistemas de información y componentes tecnológicos.

c. Los repositorios o almacenamientos donde se guarden los registros de auditoría deben estar protegidos contra accesos y modificaciones no autorizados. Las

actividades de usuarios operadores y administradores en los sistemas de procesamiento de información o sus componentes deben ser objeto del monitoreo.

d. La Gerencia de Tecnología debe garantizar que todos los relojes de sistemas de información, aplicaciones y componentes tecnológicos estén sincronizados con al menos una fuente segura de la hora legal colombiana.

e. Los registros de auditoría (logs) deben almacenar como mínimo la información de identificación del usuario, el origen o dirección IP, la fecha y hora del evento, la descripción del evento y su estado de éxito.

3.5.8. Integridad del software productivo

Todo software que se ejecute en los equipos de cómputo de ÁGATA debe originarse de fuentes confiables, para evitar alteraciones no autorizadas. La Gerencia de 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.

El Área de Seguridad de la Información en Ágata debe establecer políticas y lineamientos asociados al ciclo de vida del desarrollo de software seguro, aplicable a desarrollos internos o fábricas de software externas.

La Gerencia de Tecnología debe definir los procedimientos asociados al ciclo de vida del desarrollo de software que garanticen la integridad del software generado, separación de ambientes, el uso de los datos con respecto a las pruebas generadas y el cumplimiento de los lineamientos y políticas definidos para tal fin.

3.5.9. Gestión de vulnerabilidades técnicas

La Gerencia de Tecnología 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 ÁGATA. 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 de la Gerencia de Tecnología:

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 clasificadas como críticas y altas, y aquellas que sean identificadas en los activos críticos.

f. Debe fijarse un plazo máximo de tratamiento de las vulnerabilidades de tres (3) meses.

g. Debe considerarse si las acciones para remediar las vulnerabilidades son viables frente al riesgo de su implementación, y en caso de no serlo, deben definirse e implementarse controles compensatorios para mitigar los riesgos derivados de su materialización.

3.5.10. Uso de servicios en la nube

a. La Gerencia de Tecnología debe aplicar la metodología para la gestión de riesgos de seguridad de la información definida en Ágata para identificar, evaluar y tratar los riesgos asociados con el uso de servicios en la nube.

b. La Gerencia de Tecnología, como encargada de la contratación de servicios tecnológicos, debe garantizar que los contratos con los proveedores de servicios en la nube incluyen los objetivos, cláusulas, requisitos y criterios de seguridad necesarios para garantizar la privacidad, confidencialidad, integridad y disponibilidad de la información.

c. La Gerencia de Tecnología debe garantizar la identificación de roles y responsabilidades relacionadas con el uso y gestión de los servicios en la nube.

d. La Gerencia de Tecnología debe verificar la efectividad de los controles, interfaces y gestión de cambios en los servicios en nube por parte de los proveedores de servicio.

e. La Gerencia de Tecnología debe monitorear, revisar y evaluar los indicadores de disponibilidad del servicio y la gestión de los riesgos e incidentes de seguridad de la información en servicios en nube por parte de los proveedores de servicio.

3.5.11. 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 y sus condiciones de seguridad 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. La Gerencia de Tecnología debe garantizar que los sistemas de procesamiento y almacenamiento de información, los sistemas operativos y las aplicaciones de Ágata cuentan con las últimas versiones estables emitidas por los fabricantes, con el fin de dar el aseguramiento adecuado. Si estos no pueden ser actualizados, se debe documentar la excepción y el plan de gestión de riesgos derivados.

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

3.6. Seguridad en las comunicaciones

3.6.1. Seguridad de las redes

a. Las redes de ÁGATA deben contar con controles perimetrales que permitan identificar, permitir o restringir y monitorear todo el tráfico entrante y saliente hacia redes públicas, desconocidas o inseguras.

b. La administración de los controles perimetrales debe mantener registro de las autorizaciones y modificaciones realizadas con fines de auditoría.

c. En modelos distribuidos en los que no existen redes corporativas centralizadas los controles perimetrales deben implementarse en los equipos de cómputo y plataformas que estén conectados directamente a redes públicas no controladas o a Internet.

d. Se deben implementar, en la red o en los equipos de cómputo, controles para detectar y prevenir intrusiones de manera oportuna.

e. El acceso a recursos y servicios ubicados en la red de ÁGATA y que no hayan sido clasificados como públicos debe realizarse a través de tecnologías que permitan autenticar, autorizar y mantener el tráfico seguro.

f. Cada recurso o servicio de ÁGATA debe ser accedido únicamente por los usuarios que lo requieran para la ejecución de sus responsabilidades con la agencia, incluso si estos se encuentran ubicados en diferentes centros de datos en tierra o diversas nubes públicas y privadas.

g. Las interconexiones que se realicen entre las redes de ÁGATA y las redes de proveedores o clientes deben contar con controles que eviten la suplantación de cualquier extremo y el acceso a información en tránsito, y que permitan el control y monitoreo del tráfico que fluye entre las redes previa autorización para garantizar que las redes de ÁGATA y su contraparte se mantienen seguras.

h. Las redes de ÁGATA deben contar con mecanismos de segmentación, aislamiento y acceso acordes a la sensibilidad de la información.

i. El tráfico de información debe realizarse a través del uso de protocolos considerados seguros. En casos en donde por restricciones tecnológicas no se puedan reemplazar protocolos inseguros, se deben implementar capas adicionales de protección para mantener la confidencialidad e integridad de los datos.

3.6.2. Correo electrónico

a. El uso del correo electrónico, servicio de mensajería Web y demás recursos que comprenden los paquetes de colaboración (calendario, gestión de tareas, entre otros), es proporcionado por ÁGATA a trabajadores y terceros que lo requieren para el cumplimiento de sus responsabilidades laborales o contractuales. Todo usuario 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. ÁGATA 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.

c. ÁGATA es el único dueño del correo electrónico corporativo por lo que la Gerencia de Tecnología o el área o personal que dicha gerencia designe para tal fin tiene la facultad de acceder, monitorear y supervisar las cuentas de correo electrónico corporativo.

d. La Gerencia de Tecnología debe garantizar la implementación, mantenimiento y operación segura del servicio de correo electrónico, incluyendo las

configuraciones en otros sistemas para asegurar que los correos legítimos de la agencia no son considerados spam por otros servicios de correo.

e. La Gerencia de Tecnología o el proveedor que designe para la operación del servicio de correo electrónico deben monitorear continuamente que este servicio no sea reportado en listas negras de Internet y realizar las acciones requeridas para retirarlo de las listas en caso de ser identificado como spam.

f. Los usuarios del servicio de correo electrónico pueden enviar información sensible a través de este servicio únicamente si garantizan que la información es adjuntada y protegida mediante el uso de algoritmos sólidos de criptografía. El envío de las credenciales o elementos para descifrar la información debe realizarse a través de otros medios diferentes al correo electrónico.

g. El reenvío automático de cuentas de ÁGATA a cuentas de correo electrónico personales o públicas está prohibido.

h. Sólo es permitido tener copias locales del correo electrónico de ÁGATA en equipos de cómputo de la agencia previa autorización del Área de Seguridad de la Información y con los procedimientos establecidos y ejecutados por la Gerencia de Tecnología.

i. La configuración y uso de relays de correo electrónico para el envío masivo de mensajes debe estar justificado en una necesidad de negocio y contar con la aprobación del área encargada de la Seguridad de la Información. La Gerencia de Tecnología debe garantizar la configuración requerida para evitar que los correos electrónicos enviados sean identificados como spam y para asegurar que el envío se realiza únicamente por personas o sistemas debidamente identificados y autorizados.

3.6.3. Uso de internet y de la red interna

a. ÁGATA, a través de la Gerencia de Tecnología provee acceso a Internet en sus instalaciones con el objetivo de facilitar el logro de la misión. En consecuencia, todos los usuarios deben acogerse a los lineamientos de esta política.

b. ÁGATA se reserva el derecho de restringir el acceso a sitios y aplicaciones web que puedan afectar la productividad, la seguridad de su información o su personal. Estas restricciones aplican a todos los equipos conectados a redes corporativas de Ágata o a los equipos de Ágata que estén conectados a Internet a través de otros canales de comunicaciones.

c. Los usuarios deben abstenerse de visitar sitios restringidos por ÁGATA de manera directa o indirecta.

d. La Gerencia de Tecnología puede registrar y monitorear toda actividad relacionada con la navegación en Internet con el propósito de monitorear y mejorar los niveles del servicio y mantener los niveles de seguridad de la infraestructura tecnológica y la información. ÁGATA 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 encargada de la Seguridad de la Información.

f. Los sitios y aplicaciones web permitidos por Ágata deben ser utilizados por los usuarios con las cuentas y credenciales corporativas. Se debe evitar el acceso mediante otras cuentas personales o corporativas, privadas o públicas.

g. El Área de Seguridad de la Información debe capacitar a los funcionarios de la Agencia sobre el uso seguro y apropiado de los recursos en línea, incluyendo el acceso a red.

3.7. Adquisición y desarrollo de sistemas

a. La Gerencia de Tecnología es la única área de Ágata autorizada para comprar, desarrollar, implementar, mejorar u operar software y hardware, misional o de apoyo, para uso interno o externo. Una o varias responsabilidades pueden ser tercerizadas a través de proveedores idóneos para cumplirlas.

b. El software que se requiera en Ágata puede ser adquirido o desarrollado por personal propio o por un tercero según se obtenga mejor relación utilidad, funcionalidad, costo y tiempo.

c. Los procesos de selección de software deben incluir dentro del análisis el cumplimiento de requerimientos de seguridad asociados a la gestión de la información que se espera gestionar en ellos, al desarrollo y construcción de estos, a la infraestructura tecnológica que los soporta y a la seguridad en su mantenimiento y operación.

d. Cualquier modificación sobre un sistema de información existente debe incluir la identificación de requerimientos de seguridad en conjunto con los requerimientos funcionales y pasando por el respectivo proceso de gestión de cambios.

e. Todo componente nuevo o que forme parte de un cambio en un sistema de información debe pasar previamente por un proceso de pruebas funcionales que certifique su correcta operación antes de ser puesto en marcha. Si se considera que el cambio afecta los niveles de seguridad del sistema, se deben realizar

pruebas de seguridad que validen el cambio unitario y la seguridad general del sistema.

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

g. El desarrollo de software en ÁGATA, sea directo o a través de terceros, debe realizarse mediante un proceso de desarrollo seguro de software que involucre a todos los actores involucrados en la protección y aseguramiento de la información.

h. Todos los desarrollos y piezas de software deben responder a requerimientos previamente definidos y autorizados. No se deben crear, modificar o actualizar rutinas, funciones u operaciones que tengan comportamiento de virus, puertas traseras o malware.

i. Todos los desarrollos deben ser sometidos a pruebas de seguridad en búsqueda de vulnerabilidades o comportamientos maliciosos. Sólo pueden pasar a producción cuando hayan pasado exitosamente todas las pruebas.

3.8. Proveedores

3.8.1. Relación con proveedores

a. La Gerencia de Asuntos Corporativos debe identificar y documentar los tipos de proveedores, las relaciones existentes con ellos y los privilegios con que están autorizados a consultar información de ÁGATA o cualquiera de sus clientes. Del mismo modo deben documentarse los privilegios asignados a ÁGATA si es la agencia la que accede a la información de los proveedores.

b. La Gerencia de Asuntos Corporativos debe definir los procesos asociados a un ciclo de vida estandarizado para administrar las relaciones con los proveedores.

c. La Gerencia de Asuntos Corporativos debe plasmar en cada acuerdo contractual con proveedores los requerimientos de seguridad de la información y de protección de datos personales requeridos para cada parte con el propósito de garantizar la seguridad de la infraestructura y de la información contenida en ella. Los requerimientos deben ser acordados con las áreas internas involucradas.

d. La Gerencia de Asuntos Corporativos debe establecer procedimientos para monitorear el cumplimiento de los requerimientos de seguridad de información establecidos para cada tipo de proveedor y tipo de acceso.

e. Los requerimientos de seguridad de la información y las consecuencias de su incumplimiento deben ser parte integral de los acuerdos contractuales.

f. El Área de Seguridad de la Información debe definir programas de capacitación y concienciación para el personal de ÁGATA que interactúa con el personal de proveedores, sobre sus obligaciones y uso aceptable de la información y los recursos informáticos de ÁGATA a los que tenga acceso.

g. 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.

h. 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.

i. Los procesos, servicios o herramientas tecnológicas que los proveedores prestan a Ágata deben contar con evaluaciones independientes de seguridad que garanticen sus niveles de cumplimiento de estándares aplicables o de las políticas de seguridad de la información de Ágata.

3.8.2. Acuerdos contractuales

Los acuerdos contractuales con proveedores son vitales para garantizar los niveles de protección de la información y de la infraestructura de Ágata, por tal razón, la Gerencia de Asuntos Corporativos debe seguir los siguientes lineamientos:

a. En los contratos con los proveedores se debe contemplar que estos se acojan y cumplan las políticas, lineamientos, procedimientos y en general toda la documentación de Ágata relacionada con el 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 ÁGATA le confía con los más altos estándares de confidencialidad, integridad y disponibilidad.

c. Los acuerdos contractuales con proveedores deben garantizar el aislamiento de la información de ÁGATA respecto de otra información que pueda tener el proveedor en custodia o tratamiento de otros clientes.

d. Los proveedores deben tener la responsabilidad contractual de informar oportunamente a ÁGATA sobre la ocurrencia de incidentes de seguridad de la información y de colaborar durante su remediación.

e. Los acuerdos contractuales deben incluir la obligación del proveedor de establecer las contingencias necesarias para continuar con la gestión de información que ÁGATA le ha confiado ante eventos adversos no planeados.

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 ÁGATA 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 cuando sea aplicable.

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 ÁGATA. Así mismo el contrato o acuerdo debe cumplir con todos los requisitos exigidos en el artículo 2.2.2.25.5.2. del Decreto 1074 de 2015.

h. Cuando un proveedor subcontrate otros proveedores para cumplir con los acuerdos establecidos con ÁGATA debe exigirse contractualmente la necesidad de conocer la cadena de subcontratación, 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 donde se alojarán los datos confiados por ÁGATA.

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 ÁGATA 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. El personal contratado por el proveedor que realice funciones para ÁGATA debe contar con estudios de seguridad pertinentes a la clasificación de la información a la que acceden.

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. Los acuerdos contractuales deben incluir el derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo por parte de ÁGATA o un tercero que la agencia disponga para tal fin.

3.8.3. Monitoreo y revisión de los servicios contratados

a. Cada contrato debe contar con una persona o equipo de administración de contratos y con un responsable funcional quienes en conjunto tienen la responsabilidad de administrar las relaciones con el proveedor y garantizar el cumplimiento de las obligaciones del presente numeral.

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 requieran los acuerdos.

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

3.9. Gestión de incidentes de seguridad de la información

3.9.1. 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.

b. Ágata debe propender por hacer parte activa de una organización dedicada a la respuesta ante emergencias informáticas (CERT o CSIRT por sus siglas en inglés) con el propósito de recibir apoyo logístico e información relacionada con incidentes propios, del sector y de la región.

Se deben establecer procedimientos, alineados con el marco general de protección de datos personales según la Política de Tratamiento de Datos de Ágata, para:

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

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

e. Registrar actividades de administración de incidentes.

f. Administrar y guardar evidencia forense.

g. 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.

h. La respuesta, incluido el escalamiento, la recuperación controlada desde un incidente y la comunicación a las personas internas y externas u organizaciones.

i. El reporte del incidente ante el organismo de control del régimen de protección de datos personales, según aplique.

3.9.2. 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

j. Indicios de compromiso de aplicaciones, sistemas o recursos

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

3.9.3. Evidencia y evaluación

a. El tratamiento de los incidentes de seguridad prima sobre cualquier otra acción, incluso aquellas encaminadas al restablecimiento de la operación, ya que estas pueden dañar evidencia necesaria para el análisis del incidente actual y la prevención de incidentes futuros.

b. Se deben evaluar los eventos de seguridad de la información y se deben decidir si se clasifican 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.

c. 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.

d. 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.

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

3.9.4. 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.

i. Incluso si no se han materializado incidentes de seguridad, el equipo de gestión de incidentes debe realizar al menos una prueba anual mediante la simulación de cada tipo de incidente con el propósito de mantener presente los procedimientos de gestión, evaluar su efectividad y proponer mejoras que puedan facilitar la gestión de un incidente real.

3.10. 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 ÁGATA deba operar en contingencia ante situaciones adversas, es decir durante una crisis o desastre. Por tal razón se deben definir e implementar controles de seguridad de la información equivalentes a los de los ambientes productivos en los ambientes de contingencia.

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 ÁGATA administra un desastre y mantiene la seguridad de su información en el nivel definido.

f. Se debe verificar mínimo dos (2) veces al año la validez 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 donde se almacena y procesa información de ÁGATA. 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.

3.11. 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 ÁGATA y para cada sistema donde se almacene o procese información. Por lo mismo deben considerarse estos requisitos de manera explícita en los acuerdos que se establezcan con terceros donde se involucren sistemas de información.

3.11.1. Seguridad de las bases de datos con información personal

De acuerdo con la legislación vigente, Agata debe designar un Oficial de Protección de Datos, quien además de cumplir con sus obligaciones descritas en la Política de Tratamiento de Datos Personales de Ágata, debe garantizar el cumplimiento de los siguientes lineamientos de seguridad de la información:

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, estas sólo 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. La información personal debe ser objeto de auditorías periódicas que permitan identificar oportunidades de mejora en su tratamiento, que contribuya 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 clientes, proveedores, contratistas o terceros para fines comerciales o beneficios personales o de terceros, 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 ÁGATA aquellos datos que sean estrictamente necesarios para los fines de su uso.

i. Toda actividad de consulta o modificación de información considerada dato personal debe dejar trazas de auditoría de acuerdo con las políticas del presente documento, numeral 2.5.7.

j. La implementación de un Programa de Protección de Datos Personales o de un Sistema de Gestión de Privacidad debe estar alineada con los requerimientos de seguridad de la información definidos en la presente política o en cualquier otro documento que haga parte de su marco de gobierno corporativo. Se debe propender porque la gestión de riesgos de seguridad de la información y de privacidad se realice a través de un sistema integrado de gestión de riesgo.

3.11.2. Enmascaramiento de datos personales

a. En los acuerdos contractuales de transferencia o transmisión de información se debe garantizar que existan cláusulas que especifiquen los requisitos de anonimización o seudonimización con el objetivo de garantizar que los datos no puedan técnicamente ser asociados con los titulares de la información.

b. Si en los acuerdos de transferencia o transmisión de información se acuerda que los datos personales son entregados a Ágata en claro, la Agencia debe definir y aplicar procedimientos para ajustarlos, limpiarlos, estandarizarlos, homologarlos y anonimizarlos antes de ser tratados. Si la funcionalidad para la cual se deben utilizar los datos requiere relación con los titulares, se deben plantear procedimientos de seudonimización que permitan desanonimizarlos únicamente en las fases que se requiera y para usuarios con la autorización correspondiente.

c. Ágata debe garantizar la trazabilidad de los datos personales, estén anonimizados, seudoanimizados o en claro, para identificar inequívocamente los usuarios y las acciones realizadas sobre ellos.

d. Se debe verificar que las técnicas de enmascaramiento de datos, seudonimización o anonimización utilizadas por Ágata cumplan con los criterios más seguros definidos por la industria con el fin de reducir el riesgo de reasociación de los datos con sus titulares.

3.11.3. 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 ÁGATA, 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 transgrede 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 ser realizadas únicamente por la Gerencia de Tecnología y contar con el aval del líder pertinente en ÁGATA.

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.

3.11.4. Auditorías de seguridad y privacidad 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 ÁGATA.

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 ÁGATA.

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. Los líderes de área deben identificar y verificar que se cumplen los requisitos y estándares 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 donde se almacena y procesa información se deben auditar 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 cuán eficaces son los controles para evitar el acceso no autorizado debido a estas vulnerabilidades.

Control de Cambios

Versión	Fecha	Descripción del cambio	Aprobado por
1.0	Noviembre 20 de 2020	Documento inicial	Manuel Riaño – Líder Proyecto para la constitución de La Agencia Analítica de Datos del Distrito
1.1	Septiembre de 2021	Inclusión de imagen corporativa Definición de responsabilidades	Sandra Borda - Ágata
2.	Agosto de 2022	Actualización y reestructuración de las Políticas de Seguridad de la Información	Asamblea de Accionistas