ALCALDÍA MAYOR
DE BOGOTÁ D.C.

BOGOTÁ | ATENEA

RESOLUCIÓN 140 **DE** 04 de octubre de 2022.

"Por medio de la cual se adopta la política de seguridad y privacidad de la información en la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología —Atenea"

EL DIRECTOR GENERAL

En uso de las facultades legales establecidas en la Ley 489 de 1998, articulo 2.2.2.2.1 del Decreto 1083 de 2015 y en especial las conferidas por el artículo 11 del Decreto Distrital No. 273 de 2020 y

CONSIDERANDO

Que la Constitución Política de 1991, estableció en el artículo 15 la protección de la información y de los datos personales, y lo eleva como derecho fundamental de todas las personas a conservar su intimidad personal y familiar, al buen nombre, a conocer, actualizar y rectificar, las informaciones que hayan recogido sobre ellos, en bancos de datos y archivos de las entidades privadas y públicas.

Que Ley 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."* , estableció los lineamientos necesarios para que los organismos públicos y privados identificaran los roles y la tipología de datos que son objeto de protección constitucional, así mismo, dispuso las condiciones en las cuales se deben recolectar los datos personales que posteriormente serán vinculados con la administración de una base de datos.

Que la Ley 1581 de 2012, "*Por la cual se dictan disposiciones generales para la protección de datos personales",* estableció como objeto "(...) *desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma*".

Que el artículo 3 ídem define el responsable del tratamiento de datos como la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos. En ese orden, el artículo 17 ibidem, establece los deberes de los responsables del tratamiento de la información

Que la 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"* define en su artículo 1, que "*el objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información."*

Que el artículo 2.2.22.2.1 del Decreto 1083 de 2015, Único Reglamentario del Sector Función Pública, establece *"Las políticas de Desarrollo Administrativo de que trata la Ley 489 de 1998, formuladas por el Departamento Administrativo de la Función Pública y los demás líderes, se denominarán políticas de*

Gestión y Desempeño Institucional y comprenderán, entre otras, las siguientes: (...)11. Gobierno Digital, antes Gobierno en Línea. 12. Seguridad Digital (…)".

Que el artículo 2.2.9.1.1.3. del Decreto 1078 de 2015, Nacional Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, establece que *"(…)la política de Gobierno Digital se desarrollará conforme los principios que rigen la función pública y los procedimientos administrativos consagrados en los Artículos 209 de la Constitución Política, 3 de la Ley 489 de 1998, 3 de la Ley 1437 de 2011, 2 y 3 de la Ley 1712 de 2014, así como los que orientan el sector TIC establecidos en el Artículo 2 de la Ley 1341 de 2009, y en particular los siguientes"*

Que el Decreto 1074 de 2015, Único Reglamentario del Sector Comercio, Industria y Turismo, en su artículo 2.2.2.25.3.1., indicó que "*Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas. Las políticas de tratamiento de la información deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares (…)".*

Que, a su vez, el parágrafo del artículo 16 del Decreto Nacional 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de tecnologías de la Información y las Comunicaciones.

Que el Ministerio de Tecnologías y las Comunicación, expidió la Resolución 00500 de 10 de marzo de 2021, donde se establecen los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital y, establece los lineamientos y estándares para la estrategia de seguridad digital, a los sujetos obligados señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015.

Que el artículo 5 de la mencionada Resolución establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos del artículo 2.2.22.3.14 del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue. Así como, adoptar el Modelo de Seguridad y Privacidad de la Información -MSPI señalado en el Anexo 1 de la misma Resolución, como habilitador de la política de gobierno digital.

Que el documento CONPES 3995 formula la Política Nacional de Confianza y Seguridad Digital en la República de Colombia, estableciendo medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, fortaleciendo las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; actualizando el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

Que la Ley 527 de 1999, define la firma digital "como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y

al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación".

Que el artículo 2.2.2.47.1. del Decreto 1074 de 2015 *"por medio del cual se expide el Decreto único Reglamentario del Sector Comercio, Industria y Turismo"*, define la firma electrónica como: métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

Que la Alcaldesa Mayor de Bogotá D.C., en ejercicio de las facultades otorgadas por el artículo 132 del Acuerdo 761 de 2020, -Plan de desarrollo económico, social, ambiental y de obras públicas del Distrito Capital 2020-2024 "*Un nuevo contrato social y ambiental para la Bogotá del siglo XXI"*-expidió el Decreto Distrital 273 de 2020, mediante el cual se creó la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología -Atenea.

Que el Consejo Directivo de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología – ATENEA expidió el Acuerdo 02 de 2021, *"Por el cual se adoptan los Estatutos, de la Agencia Distrital para la Educación Superior, la Ciencia y Tecnología -Atenea- y se dictan otras disposiciones*" donde se establece la organización y funcionamiento de la Agencia.

Que el Consejo Directivo de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología – ATENEA expidió el Acuerdo 03 de 2021, "*Por el cual se adopta la estructura organizacional, de la Agencia Distrital para la Educación Superior, la Ciencia y Tecnología -Atenea- y se dictan otras disposiciones"*.

Que de acuerdo con las normas citadas, corresponde a la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología —Atenea adoptar la Política General política de seguridad y privacidad de la información con el objetivo de proveer un ambiente seguro en el tratamiento de la información, preservando sus características esenciales de Confidencialidad, Integridad, Disponibilidad y Privacidad.

Que la Política de Seguridad y Privacidad de la Información, al interior de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología —Atenea fue revisada y aprobada por el Comité Institucional de Gestión y Desempeño en sesión realizada el día tres (03) de junio de 2022.

Que, en mérito de lo expuesto,

RESUELVE

Artículo 1. ADOPCIÓN DE LA POLÍTICA. Adóptese la Política de Seguridad y Privacidad de la Información, que se encuentra anexa al presente acto administrativo y hace parte integral del mismo.

Artículo 2. ÁMBITO DE APLICACIÓN. La presente política aplica a todos las personas naturales y jurídicas que tengan algún vínculo laboral o contractual con la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología -Atenea- y que en el ejercicio de sus actividades y/o funciones deban recolectar datos personales para ser ingresados a las bases de datos de la Agencia

Artículo 3. CONTROL. La Oficina de Control Interno de Gestión de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología -Atenea será la encargada de velar por el cumplimiento de las políticas de seguridad y privacidad de la información adoptadas a través de la presente resolución.

Artículo 4. PROCESO DE IMPLEMENTACIÓN. El proceso de implementación de la Política de Seguridad y Privacidad de la Información estará a cargo de las áreas definidas en el ítem -Roles y Responsabilidades que se encuentra anexo a este acto administrativo.

Artículo 5. VIGENCIA. La presente resolución rige a partir de la fecha de su publicación.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá D.C, a los 04 días del mes de octubre del 2022

GERMÁN BARRAGÁN AGUDELO
DIRECTOR GENERAL

Revisó:	Ingrid Carolina Silva Rodríguez, Jefe Oficina Asesora Jurídica Mario Alfonso Pardo Pardo – Subgerente de Planeación y Gerente de Estrategia (E) Lira Jazmín Pineda Moreno, Subgerente de Tecnologías de la Información y las Comunicaciones Karen Andrea Barrios Lozano – Abogada Contratista Hevert Steven Bernal Carvajal - Abogada Contratista Oficina Asesora Jurídica
Elaboró.	María Alejandra Suarez, Contratista Subgerencia de Tecnologías de la Información y las Comunicaciones

ALCALDÍA MAYOR
DE BOGOTÁ D.C.

BOGOTÁ | ATENEA

Política de Seguridad y Privacidad de la Información

ATENEA
AGENCIA DISTRITAL PARA LA EDUCACIÓN SUPERIOR LA CIENCIA Y LA TECNOLOGÍA

Subgerencia de Tecnologías de la Información y las Comunicaciones

Bogotá D.C

Contenido

INTRODUCCIÓN 7
OBJETIVO 7
OBJETIVOS ESPECÍFICOS 7
ALCANCE 7
GLOSARIO 8
MARCO LEGAL 9
POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 11
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 11
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 12
ROLES Y RESPONSABILIDADES 12
COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO 12
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN 12
SUBGERENCIA DE PLANEACIÓN 13
LÍDERES DE PROCESO Y EQUIPOS DE TRABAJO 13
SUBGERENCIA DE TECNOLOGÍAS DE INFORMACIÓN Y LA COMUNICACIÓN 13
SUBGERENCIA DE GESTIÓN ADMINISTRATIVA 13
OFICINA ASESORA JURÍDICA 14
OFICINA DE CONTROL INTERNO 14
OFICINA DE CONTROL INTERNO DISCIPLINARIO 14
GESTIÓN DE ACTIVOS DE INFORMACIÓN 14
CONTROL DE ACCESO 15
CRIPTOGRAFÍA 16
SEGURIDAD FISICA Y DEL ENTORNO 16
SEGURIDAD DE LAS OPERACIONES 16
SEGURIDAD DE LAS COMUNICACIONES 17
DESARROLLO Y MANTENIMIENTO DE SISTEMAS 17
RELACIÓN CON LOS PROVEEDORES 17
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO 18
CUMPLIMIENTO 18
VIGENCIA 18

INTRODUCCIÓN

La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea", con el objetivo de cumplir las normativa y legislaciones que le aplican a las Entidades del Estado y, para preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona en los procesos y a través de los procedimientos, debe aplicar políticas de seguridad que minimicen los riesgos que amenacen y vulneren la información, con el fin de dar continuidad en su gestión.

Para ello, la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" consciente de la importancia de definir estos controles, ha desarrollado un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con los objetivos estratégicos de la Entidad, planteando así las políticas, lineamientos y responsabilidades de todos los funcionarios, contratistas y terceros que intervengan en la generación, tratamiento y almacenamiento de la información.

OBJETIVO

Definir directrices y lineamientos que faciliten los mecanismos para proteger los activos de información donde se administre, produzca, procese y/o transforme la información de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" ante cualquier amenaza que pueda comprometer la confidencialidad, disponibilidad e integridad de esta información.

OBJETIVOS ESPECÍFICOS

- Gestionar los riesgos de seguridad de la información de forma oportuna por medio de controles, ayudando a reducir los impactos negativos de su materialización.
- Reducir los incidentes de Seguridad de la Información que afecten el normal funcionamiento de la entidad.
- Fomentar una cultura y apropiación de seguridad y privacidad de la información en los colaboradores de la Agencia frente al Sistema de Gestión de Seguridad de la Información -SGSI.

ALCANCE

La Política General de Seguridad y Privacidad de la información aplica para todos los procesos, sedes, colaboradores (funcionarios y contratistas) y terceros de La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea", y demás actores que tengan acceso a sus instalaciones y/o servicios tecnológicos.

GLOSARIO

Activo de información: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
Amenaza: causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.
Análisis de riesgos: proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
Anonimizar el dato: eliminar o sustituir algunos nombres de personas (naturales o jurídicas); direcciones y demás información de contacto que no sea de carácter público.
Autenticidad: propiedad de que una entidad es lo que afirma ser. (ISO 27000).
Ciberespacio: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).
Colaborador: Empleado, contratista, practicante, proveedor y en general cualquier persona que tenga acceso a información de la Agencia y tenga un vínculo contractual con el mismo.
Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Control: comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.
Custodio de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la Veeduría Distrital, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.
Dato público: es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.
Disco duro: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.
Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.
Gestión de incidentes de seguridad de la información: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Gestión de riesgos: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
Habeas data: derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.
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.

Información: La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.
Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.
Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000)
Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.
No repudio: 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). (ISO-7498-2).
Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
Propietario de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.
Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones.
Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.
Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.
Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sea asociada de modo inequívoco a un individuo o entidad.
Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000).

MARCO LEGAL

- Ley 1273 de 2009 del Congreso de la República. 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.

- Ley 1581 de 2012 del Congreso de la República. Por el cual se dictan disposiciones generales para la protección de datos personales.

- Ley 1712 de 2014 del Congreso de la República. 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.

- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos

- Decreto 316 de 2008 de la Alcaldía Mayor de Bogotá D.C. Por medio del cual se modifica parcialmente el artículo 3° del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico.

- Decreto 2609 de 2012 de la Presidencia de la República. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

- Decreto 1377 de 2013 de la Presidencia de la República. Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.

- Decreto 2573 de 2014 de la Presidencia de la República. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

- Decreto 103 de 2015 de la Presidencia de la República. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.

- Decreto Único Reglamentario 1078 de 2015, Título 9 capítulo 1, Estrategia del Gobierno en Línea. Sección 2, Artículo 2.2.9.1.2.1 numeral 4 define el componente de Seguridad y Privacidad de la Información.

- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado

- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

- Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

- CONPES 3854 de 2016. Política Nacional de Seguridad digital.

- Norma Técnica ISO/IEC 27001 de 2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea", entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el cumplimiento de la normatividad vigente y en concordancia con la misión y visión de la entidad.

Para la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea", la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones y toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los ciudadanos, colaboradores y demás entidades.
- Apoyar la innovación tecnológica.
- Proteger los activos de información
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea"
- Garantizar la continuidad de TI frente a incidentes.
- La Agencia, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

La Agencia, considerará como información aquella que se maneje en virtud de los procesos de la Entidad y de los proyectos de inversión.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea",

- Ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Establece las responsabilidades frente a la seguridad de la información, las cuales serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas o terceros.
- Protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio y proyectos de inversión, con el fin de minimizar impactos financieros, operativos o legales

debido a un uso incorrecto de la misma. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- Protegerá su información institucional de las amenazas originadas por factores internos y externos que afecten cualquiera de sus principios.
- Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementará control de acceso a la información, sistemas y recursos de red.
- Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- Garantizará la confiabilidad y el nivel de sensibilidad de la información que provenga de terceros y de sistemas de información con los cuales se tenga interoperabilidad.
- Actualizará la política teniendo en cuenta la valoración de riesgos de procesos y de seguridad de la información.
- En caso de incumplimiento de las Políticas de Seguridad y Privacidad de la información, la Entidad, iniciará las investigaciones disciplinarias correspondientes, conforme a lo dispuesto en la Ley 734 del 2002.

A continuación, se relacionan los lineamientos para la aplicación de la política especifica de seguridad y privacidad de la información

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" definió en el documento “Roles y Responsabilidades de Seguridad de la Información”, los diferentes actores con sus funciones en materia de Seguridad de la Información en la Entidad.

ROLES Y RESPONSABILIDADES

A continuación, se describen los roles y responsabilidades de la seguridad de la información para la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea":

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

Representante de la alta dirección, el cual es la Instancia encargada de realizar la revisión, seguimiento y aprobación de la implementación, mantenimiento y mejora continua del Sistema de Gestión de seguridad de la Información - SGSI.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Responsable de presentar al Comité Institucional de Gestión y Desempeño la documentación, estrategias y propuestas para el mantenimiento y fortalecimiento del SGSI, así como liderar la implementación, mantenimiento y mejora de este con el fin de fomentar una cultura de la seguridad de la información en Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea".

Definir e implementar las políticas y controles de Seguridad de la información.

SUBGERENCIA DE PLANEACIÓN

Responsable de asesorar a las áreas en la realización de los cambios a que haya lugar en los procesos, procedimientos, instructivos y formatos de la Entidad para ajustarlos y alinearlos con el Modelo Integrado de Planeación y Gestión -MIPG, el Sistema de Gestión de Seguridad de la Información – SGSI, así como apoyar el proceso de su documentación.

LÍDERES DE PROCESO Y EQUIPOS DE TRABAJO.

Cumplir con las políticas, lineamientos, procesos, procedimientos y asistir a las sensibilizaciones o capacitaciones programadas por el Sistema de Gestión de seguridad de la información SGSI.

Son responsables de velar por la protección de los activos de información y controlar la producción, desarrollo, mantenimiento, uso, seguridad y actualización de estos.

SUBGERENCIA DE TECNOLOGÍAS DE INFORMACIÓN Y LA COMUNICACIÓN

- Implementar las políticas y controles de Seguridad informática
- Gestionar los incidentes de seguridad informática
- Supervisar las acciones de mejora continua en el Sistema de Gestión de Seguridad de la Información -SGSI.
- Proponer al Comité Institucional de Gestión y Desempeño la política Institucional de seguridad y privacidad de la información y coordinar su implementación a través del Oficial de Seguridad
- Monitorear el cumplimiento de los linimentos definidos en la política institucional de seguridad y privacidad de la información.
- Definir e implementar la estrategia de continuidad para los servicios tecnológicos.
- Presentar al Comité Institucional de Gestión y Desempeño el resultado de los resultados obtenidos en la implementación de la política de seguridad y privacidad de la información.

SUBGERENCIA DE GESTIÓN ADMINISTRATIVA

Encargado de:

- Coordinar la seguridad y los accesos físicos en la Agencia.
- Verificar el cumplimiento de la presente política en la gestión de todos los contratos u acuerdos de la Agencia con colaboradores o terceros.
- Gestionar los activos físicos de la entidad a través de procedimientos y lineamientos
- Atender los incidentes y eventos de seguridad que se presenten en los activos de información físicos.
- Atender, gestionar y direccionar las PQRSD que lleguen a la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" dentro de los términos legales vigentes. Responsable de dar a conocer al ciudadano las políticas del Sistema de Gestión de Seguridad de la Información – SGSI.

- Incluir las cláusulas de seguridad de información en los contratos y verificación de los acuerdos de niveles de servicio; dictar lineamientos para que se reporte oportunamente el retiro de colaboradores.

  La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" consignará como obligación general en todos los contratos el siguiente texto:

"*Mantener reserva sobre la información que tenga acceso con ocasión del cumplimiento de las obligaciones contractuales. En este sentido EL CONTRATISTA deberá abstenerse de publicitar o utilizar información que se le entregue, como resultado del desarrollo del contrato*."

"Conocer y dar cumplimiento de las políticas que componen el Sistema de Gestión de Seguridad de la Información – SGSI"

Todo funcionario y/o contratista que ingrese a la Entidad, debe leer y firmar el compromiso de manejo de la información y tratamiento de datos personales, anexo a esta política.

- Coordinar y ejecutar los programas de Inducción y Reinducción dentro del Plan Institucional de Capacitación, donde se comunicará a los servidores públicos y contratistas los lineamientos de seguridad de la información, las obligaciones respecto al cumplimiento de las políticas de seguridad y privacidad de la información y la protección de datos personales.

OFICINA ASESORA JURÍDICA

Realizar la asesoría legal frente al cumplimiento de la normatividad relacionada con la seguridad de la información, protección de datos personales, transparencia y acceso a la información pública, entre otras. Responsable de asesorar en materia legal a la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" en temas de seguridad de la información.

OFICINA DE CONTROL INTERNO

Responsable de evaluar y realizar seguimiento al cumplimiento de las políticas, planes y requisitos de Seguridad de la información, auditar el SGSI y presentar los hallazgos.

OFICINA DE CONTROL INTERNO DISCIPLINARIO

Llevar a cabo las investigaciones necesarias por incumplimiento de los lineamientos y políticas definidas en seguridad de la información para la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea"

GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" con el liderazgo de la Dirección y el trabajo articulado de la Subgerencia de Tecnologías de la Información y los procesos institucionales, realizarán la identificación, clasificación y etiquetado de los activos de información de La Agencia mediante la metodología que se establezca.

Los funcionarios y contratistas deberán evitar la divulgación, modificación, retiro y destrucción no autorizados de información almacenada en los medios accesibles.

Todo funcionario y contratista que se desvincule temporal o definitivamente de La Agencia deberá realizar la devolución de activos de información que tenga asignados y en custodia, físico o virtual, al supervisor o jefe inmediato, de acuerdo con los lineamientos definidos para tal fin.

La información almacenada en los portátiles es responsabilidad de quien use el equipo, la Subgerencia de Tecnologías de la Información y la Comunicación hará mantenimiento a dichos equipos y eliminará los archivos en intervalos planificados.

Es de exclusiva responsabilidad de cada colaborador tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles, evitando accesos no autorizados, daños, pérdida de información o extravío del medio.

La información que reposa en los equipos portátiles asignados por la Entidad es responsabilidad de quien tiene en uso el dispositivo móvil. Cuando se entreguen estos dispositivos, el área encargada deberá eliminar los datos contenidos en el dispositivo.

La Subgerencia de Tecnologías de la Información y la Comunicación será el encargado de realizar las copias de seguridad de la información guardada en las unidades de red.

CONTROL DE ACCESO

- La creación, reactivación o desactivación de usuarios de la red o sistemas de información; al igual que los roles y permisos otorgados, los realizará la Subgerencia de Tecnologías de la Información y la Comunicación a través del procedimiento establecido para tal fin.

- La Subgerencia de Tecnologías de la Información y la Comunicación gestionará el control de acceso a través de usuario y contraseña, a la red de la Entidad, correo electrónico y a los sistemas de información que administre, para ello, diligenciará por cada usuario el formato dispuesto para tal fin.

- En caso de retiro temporal o definitivo de cualquier servidor público o contratista, se deberá deshabilitar los privilegios en los sistemas y actualizarlos en caso de encargos o suplencia temporal, previa solicitud por correo electrónico, enviada por el jefe inmediato y/o supervisor al Subgerente de Tecnologías de la Información y la Comunicación.

- La Subgerencia de Tecnologías de la Información y la Comunicación debe mantener actualizada la documentación relacionada con la administración de usuarios y monitoreará la asignación de permisos y roles otorgados a los usuarios.

- Las contraseñas serán de uso personal e intransferible, deberán ser cambiadas con frecuencia. Evitar que las contraseñas sean fáciles de recordar; no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.); no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios); estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos; si son temporales, cambiarlos la primera vez que se ingrese.

- Es responsabilidad del funcionario o contratista el uso dado a su usuario y contraseña.

- El administrador de la red configurará el servicio de autenticación para que trimestralmente el sistema solicite al usuario cambio de contraseña.

- No es recomendable el uso de la opción ‘recordar contraseña’.

- La instalación de software en los equipos de cómputo en la Agencia será realizada a través del usuario del administrador de la red. Toda solicitud al respecto debe gestionarse a través de la Subgerencia de Tecnologías de la Información y la Comunicación quien aprobará su instalación.

CRIPTOGRAFÍA

Identificar, definir e implementar los controles criptográficos para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

SEGURIDAD FISICA Y DEL ENTORNO

La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" a través de la Gerencia de Gestión Corporativa velará por:

- Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información.
- Diseñar y aplicar la protección contra desastres naturales, ataques maliciosos y accidentes para evitar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre.

SEGURIDAD DE LAS OPERACIONES

La Agencia a través de la Subgerencia de Tecnologías de la Información y las Comunicaciones velará por:

- Documentar, aplicar y poner a disposición los procedimientos de operación de los servicios tecnológicos.
- Seguimiento y gestión a los cambios en las instalaciones y sistemas de procesamiento de información que afectan la seguridad de la información.
- Separar los ambientes de desarrollo, prueba y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.
- Hacer seguimiento al uso de los recursos tecnológicos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
- Asegurarse que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
- Implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
- Hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
- Elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
- Registrar las actividades del administrador y del operador del sistema, revisándolas con regularidad.
- Sincronizar los relojes de todos los sistemas de procesamiento de información con una única fuente de referencia de tiempo.
- Implementar procedimientos para controlar la instalación de software en sistemas operativos
- Obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

SEGURIDAD DE LAS COMUNICACIONES

Asegurar la protección de la información en las redes e infraestructura de procesamiento de información, a través de documentación y controles efectivos que permitan conexiones seguras para los fines institucionalmente establecidos.

DESARROLLO Y MANTENIMIENTO DE SISTEMAS

De manera armónica durante el desarrollo y mantenimiento de los sistemas de información, se tendrán en cuenta los siguientes aspectos:

- Conocer e implementar la guía de estilo e imagen institucional en aspectos en los que aplique para el desarrollo de los sistemas de información.
- Garantizar ambientes seguros de desarrollo, pruebas y producción.
- Todo sistema de información o desarrollo de software debe poseer un plan de pruebas de calidad que incluya pruebas de seguridad.
- Especificar las carpetas y archivos a los cuales se les debe generar copias de seguridad de acuerdo con los lineamientos que defina la Oficina de Tecnologías de la Información
- Mantener actualizada la documentación de los desarrollos realizados y estándares que se emplearan.
- Establecer un plan para el análisis y tratamiento de vulnerabilidades en los sistemas de información.
- Establecer como obligación específica a los proveedores en sus contratos la entrega de la documentación necesaria para la administración y funcionamiento de los sistemas de información.
- Realizar transferencia de conocimiento, obligación específica que debe estar consignada en el contrato cuando así sea el caso.

RELACIÓN CON LOS PROVEEDORES

La Agencia debe:

- Establecer y documentar los requisitos de seguridad de la información con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la Agencia.
- Cuando sea el caso, requerir al proveedor planes de continuidad y recuperación de desastres que le permitan prestar en forma continua el servicio contratado.
- Realizar seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Agencia debe:

- Establecer las responsabilidades y procedimientos de gestión para una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. Todos los colaboradores deben reportar los incidentes de seguridad de la información a La Subgerencia de Tecnologías de la Información y la Comunicación tan pronto como tengan conocimiento de este o sospechen de alguno.

- Definir y aplicar procedimientos para preservar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información con el fin de ser usado en la reducción de la posibilidad o el impacto de incidentes futuros.

- Definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información de los incidentes de seguridad de la información que pueda servir como evidencia.

ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

La Agencia debe:

- Determinar los aspectos de la continuidad de la gestión de la seguridad de la información en situaciones adversas, durante una crisis o desastre entre ellas el cumplimiento de los requisitos de disponibilidad.

- Identificar, documentar, implementar y mejorar de manera continua los procesos y procedimientos para asegurar el nivel de continuidad requerido por la Agencia.

- Verificar a intervalos planificados los controles de continuidad implementados, validando su adecuado funcionamiento.

CUMPLIMIENTO

La Agencia debe:

- Propender la identificación, documentación y cumplimiento de las obligaciones legales, estatutarias y demás normatividad vigente relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

- Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

- Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación en materia.

- Realizar revisión del SGSI, con el fin de identificar su adecuada implementación y operación conforme a las políticas definidas.

VIGENCIA

La presente política de seguridad y privacidad de la Información cuenta con la revisión y aprobación del Comité Institucional de Gestión y Desempeño y se encuentra vigente a partir de su publicación a través de la Resolución 140 de 04 de octubre de 2022. Será revisada a intervalos planificados, o cuando se produzcan cambios significativos en los procesos, infraestructura física o tecnológica o todo aspecto que afecte la misionalidad de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea".