INTRODUCCIÓN

La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología -ATENEA- se compromete a cumplir con la normativa y legislación aplicables a las Entidades del Estado, en materia de seguridad y privacidad de la información, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información, gestionada en sus procesos y procedimientos internos y externos. Estas políticas buscan minimizar los riesgos que puedan amenazar o comprometer la información, asegurando la continuidad en la gestión de la entidad.

La información generada, custodiada o tratada en los diferentes procesos de abastecimiento de información al interior de la Agencia y con partes interesadas, es catalogada para la entidad, como activos intangibles de alto valor, por lo anterior y en consideración a su pertinencia es necesario definir, adoptar y comunicar una adecuada política de seguridad y privacidad de la información, la cual está alineada con las normas, disposiciones y tendencias que rigen en la materia.

Este enfoque integral refleja el compromiso de la Agencia ATENEA en garantizar la seguridad y privacidad de la información y promover una gestión eficaz que responda a los estándares y requisitos legales vigentes.

1. OBJETIVO DE LA POLÍTICA

Objetivo General:

Establecer directrices y lineamientos para fortalecer los mecanismos de protección de los activos de información gestionados, producidos, procesados o transformados por la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea". Estas directrices buscan salvaguardar esta información ante posibles amenazas que puedan poner en riesgo su confidencialidad, disponibilidad e integridad.

Objetivos Específicos:

- Gestionar de manera oportuna los riesgos de seguridad de la información mediante la implementación de controles, con el propósito de minimizar los impactos negativos de su materialización.
- Disminuir la ocurrencia de incidentes de Seguridad de la Información que puedan afectar el funcionamiento normal de la entidad.
- Promover una cultura de seguridad y conciencia sobre la privacidad de la información entre los colaboradores de la Agencia.
- Propiciar al interior de la entidad, el uso responsable de tecnologías modernas y adaptables a las necesidades institucionales, minimizando los riesgos asociados a los activos de información.

2. 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.

3. DEFINICIONES

- **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 Agencia ATENEA, 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**.**
- **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:** proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información**.**
- **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)
- **Inteligencia Artificial (IA):** es una rama de la informática que se centra en la creación y el uso de sistemas capaces de realizar tareas que normalmente requieren la inteligencia humana. Estas tareas pueden incluir el aprendizaje, el razonamiento, la resolución de problemas, la percepción y el uso del lenguaje. La IA puede ser utilizada en una variedad de aplicaciones.
- **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 recuperación ante desastres (DRP):** El DRP es un plan de connotación técnica, que describe cómo se deben de ejecutar diferentes acciones para reestablecer la operación de tecnologías de información y comunicaciones, después de una situación de interrupción o de crisis, catalogada como desastrosa.
  Es parte de la planificación de la continuidad del negocio y se aplica a los aspectos de una organización que dependen de una infraestructura de TI para funcionar.
- **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.
- **Propiedad intelectual (PI):** se refiere a las creaciones de la mente, como invenciones, obras literarias y artísticas, diseños, símbolos, nombres e imágenes utilizados en actividades institucionales o empresariales. La PI se protege por medio de derechos como las patentes, los derechos de autor y las marcas comerciales, que permiten a las organizaciones o personas, obtener reconocimiento o ganancias financieras por sus invenciones o creaciones. Al equilibrar el interés de los innovadores y el interés público, el sistema de PI busca fomentar un entorno propicio para la prosperidad de la creatividad y la innovación.

- **Riesgo de seguridad de la información:** 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, basado 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.
- **Tecnologías de información y comunicaciones (TIC):** Son herramientas, relacionadas con los dominios del conocimiento de la ingeniería de sistemas, electrónica, telemática o similares; que se utilizan, desarrollan y apropian en las instituciones, para mejorar y lograr efectividad y eficiencia en la ejecución de sus procesos misionales y de soportes.
  Las Tecnologías de Información y Comunicaciones (TIC) se refieren al uso de tecnologías de computación y telecomunicaciones, sistemas y herramientas para facilitar la forma en que se crea, recopila, procesa, transmite y almacena la información.

4. DESCRIPCIÓN DE LA POLÍTICA:

La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología ATENEA reconoce la importancia fundamental de gestionar de manera efectiva la información. En este sentido, se es necesario implementar medidas, controles e instrumentos para garantizar y demostrar la suficiencia en el tratamiento a los riesgos asociados a la seguridad y privacidad de la información, con el propósito de establecer un marco de confianza en el desempeño de sus responsabilidades hacia el Estado y los ciudadanos. Este compromiso se lleva a cabo en total conformidad con la normativa vigente y en coherencia con la misión y visión de la entidad.

Para la Agencia ATENEA, la protección y privacidad de los activos de información se traduce en la reducción del impacto sobre sus activos frente a los riesgos identificados. Este enfoque busca mantener un nivel de exposición que permita salvaguardar la integridad, confidencialidad y disponibilidad de la información, de acuerdo con las necesidades identificadas, de los diversos grupos de interés.

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 críticas de la entidad.
- Cumplir con los principios de seguridad y privacidad de la información.
- Adherirse a los principios de la función administrativa.
- Preservar la confianza de los ciudadanos, colaboradores y otras entidades.
- Apoyar la innovación tecnológica.
- Proteger los activos de información.
- Establecer políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en funcionarios, terceros, aprendices, practicantes y clientes de la Agencia.
- Garantizar la continuidad de las tecnologías de la información frente a incidentes.

En este contexto, la Agencia ATENEA ha decidido implementar la política de seguridad y privacidad de la información, respaldado por directrices claras alineadas a las necesidades de la entidad y los requisitos regulatorios. La definición de información incluirá aquella manejada en el contexto de los procesos de la entidad y los proyectos de inversión.

A continuación, se relacionan las directrices para la aplicación de la política de seguridad y privacidad de la información

4.1. 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 Modelo Integrado de Planeación y Gestión, entre ellos el Sistema de Gestión de seguridad de la Información – SGSI, cuando la entidad tome decisiones respecto a su implementación.

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, entre otras y asociadas a la seguridad y privacidad de la información institucional.

Subgerencia de Planeación

Responsable de apoyar a los Líderes de proceso en la realización de los cambios a que haya lugar en los procesos y la operación de la Entidad para ajustarlos y alinearlos al Modelo Integrado de

Planeación y Gestión -MIPG y al Sistema de Seguridad de la Información – SGSI, cuando la entidad tomase la decisión de su implementación, así como apoyar el proceso de su documentación.

Líderes de Proceso y Equipos de Trabajo.

Son los encargados de cumplir con las políticas, lineamientos, procesos y procedimiento del Sistema de Gestión de Seguridad de la Información SGSI. Los líderes de procesos y equipos de trabajo son los 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 las Comunicaciones

El Subgerente de Tecnologías de Información y las Comunicaciones propenderá por:

- 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 las directrices definidas en la política institucional de seguridad y privacidad de la información.
- Definir e implementar la estrategia de continuidad para los servicios tecnológicos, o el plan de recuperación ante desastres de la plataforma tecnológica.
- Presentar al Comité Institucional de Gestión y Desempeño, los resultados obtenidos en la implementación de la política de seguridad y privacidad de la información.

Subgerencia de Gestión Administrativa

El Subgerente de Gestión Administrativa propenderá por

- 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, privacidad y confidencialidad de la información, en los contratos y verificación de los acuerdos de niveles de servicio; dictar lineamientos para que se reporte oportunamente el retiro de colaboradores.
- Incorporar en el modelo de los contratos clausulas y obligaciones, sobre el cumplimiento de las políticas de seguridad, privacidad y confidencialidad sus procedimientos y los acuerdos

de confidencialidad correspondientes.

- 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.
- Definir las directrices necesarias para la implementación de la política de gestión documental de la Agencia, incluyendo la gestión de documentos electrónicos y mecanismos de firma digital, electrónica y/o complementarios; en consideración a las directrices de los organismos competentes en la materia.

Oficina Jurídica

Es la dependencia responsable de atender asuntos de carácter 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.

Oficina de Control Interno

El jefe de oficina velará por;

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

El jefe de oficina velará por;

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

4.2. Políticas Organizacionales

Gestión de Activos de Información

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

Los funcionarios y contratistas deberán evitar la divulgación, modificación, retiro y destrucción no autorizada 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 las Comunicaciones hará mantenimiento a dichos

equipos y eliminará los archivos en intervalos planificados.

La Agencia definirá el acuerdo de confidencialidad de la información, el cual debe ser adoptado por los contratistas que tengan acceso a activos de información institucional durante la ejecución contractual.

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 las Comunicaciones a través del procedimiento establecido para tal fin.
- Los encargados de la supervisión de contratistas que tengan asignación de accesos a las plataformas tecnológicas de la entidad están en la obligación, de reportar a la subgerencia de tecnologías de información y comunicaciones, cualquier novedad asociada a la suspensión y terminación contractual, con el fin que la subgerencia TIC, realice las modificaciones de accesos necesarias y requeridas.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones 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 las Comunicaciones 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 las Comunicaciones quien aprobará su instalación.

Seguridad de la información para el uso de servicios en la nube

La Agencia ATENEA velera por:

- Realizar una selección responsable de Servicios en la Nube: Únicamente proveedores de servicios en la nube que cumplan con estándares de seguridad reconocidos y que hayan sido evaluados y aprobados por la Subgerencia TIC.
- Mantener la confidencialidad de la información almacenada en la nube a través de controles de acceso sólidos y autenticación segura.
- Garantizar la integridad de los datos almacenados en la nube mediante prácticas de cifrado y medidas de seguridad contra la alteración no autorizada.
- Asegurar la disponibilidad constante de los datos y servicios en la nube mediante copias de seguridad periódicas, probadas y planes de recuperación ante desastres de la plataforma tecnológica, adecuados a las necesidades de la entidad.
- Evaluar y gestionar de forma regular los riesgos asociados al uso de servicios en la nube, implementando medidas preventivas y correctivas según sea necesario.

Los usuarios de Servicios en la Nube utilizaran exclusivamente servicios en la nube aprobados por la Subgerencia TIC.

Cumplimiento normativo, Privacidad y protección de datos personales

- Propender la identificación, documentación y cumplimiento de las obligaciones legales, estatutarias y demás normatividad vigente relacionadas con seguridad y privacidad de la información, orientada a la protección de los datos personales, de sus colaboradores, beneficiarios y partes interesadas.
- 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 registrados, patentados y los desarrollados internamente por la entidad.
- 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, al momento de su implementación, con el fin de identificar su adecuada implementación y operación conforme a las políticas definidas

Relación con los Proveedores

La Agencia debe:

- Establecer y documentar los requisitos de seguridad y privacidad 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 de negocio, certificaciones asociadas a la seguridad y privacidad de la información y planes de recuperación antes desastres; que le permitan garantizar el cumplimiento de los postulados

de confidencialidad, integridad y disponibilidad de la información, al igual que la continuidad de las operaciones de acuerdo a los acuerdos de niveles de servicios contratados.
- Realizar seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

Gestión de Eventos e Incidentes de Seguridad de la Información
La Agencia debe:

- Establecer las responsabilidades y procedimientos de gestión para una respuesta rápida, eficaz y ordenada ante los eventos e incidentes de seguridad de la información. Todos los colaboradores deben reportar los eventos e incidentes de seguridad de la información a La Subgerencia de Tecnologías de la Información y las Comunicaciones 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 los Servicios TI
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 para asegurar el nivel de continuidad requerido por la Agencia.
- Verificar a intervalos planificados los controles de continuidad implementados, validando su adecuado funcionamiento.

4.3. Política del Recurso Humano

Los funcionarios, contratistas, proveedores y cualquier persona que tenga acceso a los recursos tecnológicos y activos de información institucional deben propender por la protección, confidencialidad, integridad y disponibilidad de la información manejada, cumpliendo con los estándares:

Proceso de selección, durante y después del cargo:

- Integrar los principios de seguridad de la información en los procesos de selección y contratación.

- Establecer los acuerdos de confidencialidad y no divulgación de la información

Gestión de la Información:

- Todos los funcionarios, contratistas y cualquier persona que tenga acceso a los recursos tecnológicos son responsables de salvaguardar la información confidencial y crítica de la entidad.
- Los líderes de proceso deben fomentar una cultura de seguridad de la información y proporcionar el apoyo necesario para su implementación.

Formación y Concientización:

- Se proporcionará formación regular sobre seguridad de la información a todos los empleados.
- Todos los funcionarios, contratistas y cualquier persona que tenga acceso a los recursos tecnológicos deben estar al tanto de las políticas, normativas y procedimientos relacionados con la seguridad de la información.

Uso Apropiado de los Recursos:

- Los funcionarios , contratistas y cualquier persona que tenga acceso a los recursos tecnológicos deben utilizar los recursos de información de manera responsable y ética.
- Se deben seguir las pautas establecidas para el uso de dispositivos, sistemas y datos de la AGENCIA.

Gestión de Acceso:

- El acceso a la información estará restringido según las funciones y responsabilidades laborales.
- Se deben seguir los protocolos de autenticación y autorización para acceder a sistemas y datos sensibles.

Reporte de Incidentes:

- Todos los incidentes relacionados con la seguridad de la información deben ser reportados inmediatamente al oficial de seguridad de la información o en la mesa de ayuda de la Subgerencia TICS.

Trabajo en casa:

- Utilizar conexiones VPN seguras para acceder a los recursos de la organización desde ubicaciones remotas, en el caso de ser requeridas.
- Implementar sin excepción el doble factor de autenticación para fortalecer la autenticación y garantizar el acceso autorizado a sistemas y datos institucionales.

- Mantener actualizados los sistemas operativos y aplicaciones con los últimos parches de seguridad.
- Hacer uso de las herramientas de ofimática dispuesta por la entidad, para transferencia, comunicación y almacenamiento de la información institucional.

4.4. Políticas de control físico

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.

Así mismo desde la Subgerencia TICS

- Deberá establecer y ejecutar los planes de mantenimiento de equipos.
- Apoyará los lineamientos sobre la disposición o reutilización segura de los equipos de cómputo.

4.5. Políticas de control tecnológico

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.

Uso y aplicación de herramientas u componentes de Inteligencia Artificial – IA

La Agencia, propenderá por el uso ético y responsable de herramientas, sistemas de información o componentes tecnológicos basados en Inteligencia Artificial, para mejorar la productividad y acceso al conocimiento de sus colaboradores.

En el uso de estas herramientas y tecnologías, los colaboradores, serán responsables en todo momento por la salvaguarda de la información institucional, personal y de la protección y buen uso de los derechos de propiedad intelectual de las fuentes de datos y de información con las que interactúen y de los propios de la Agencia.

Los colaboradores de la Agencia no podrán publicar o suministrar información institucional a motores o herramientas de inteligencia artificial de tipo gratuita.

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.
- Establecer y documentar la arquitectura para sistemas de información seguros y principios de ingeniería.
- Especificar las carpetas y archivos a los cuales se les debe generar copias de seguridad de acuerdo con los lineamientos que defina la Subgerencia TICS
- 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.

Criptografía y Prevención de fuga de datos.

La entidad adoptará mecanismos de cifrado avanzados para asegurar la confidencialidad de la información, comprometiéndose a utilizar algoritmos robustos y actualizados que cumplan con los estándares de seguridad. Además, implementará un conjunto integral de medidas destinadas a prevenir la fuga de datos. Esto incluye el fortalecimiento de los controles de acceso, garantizando que solo el personal autorizado tenga acceso a información sensible, y el establecimiento de protocolos estrictos para la transferencia segura de dicha información, tanto interna como externamente.

5. VIGENCIA

La presente política de seguridad y privacidad de la Información cuenta con la revisión y aprobación del Comité Institucional de Gestión y Desempeño en sesión realizada el día tres (03) de julio de 2024 y se encuentra vigente a partir de su publicación a través de la Resolución 294 del 21 de noviembre de 2024. 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".

6. CONTROL DE CAMBIOS:

Fecha	Versión	Descripción del Cambio
04/10/2022	V1 GTI-PL-01	La política ha sido integrada conforme al formato preestablecido en el "Procedimiento de Elaboración, Modificación o Anulación de Documentos y Control de Documentos". Se actualiza la estructura de las políticas basada en la actualización de la ISO 27001:2022, en donde realiza lo siguiente: Se elimina el ítem POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN la cual se integra con la descripción de la política. Se incorpora numeral sobre Seguridad de la información para el uso de servicios en la nube y el Cumplimiento normativo, Privacidad y protección de datos personales Se estable la Política del Recurso Humano Se complementa la política de criptografía, ahora llamada Criptografía y Prevención de fuga de datos. Se incluye la política de uso de inteligencia artificial. En el año 2024 la política presenta un enfoque más integral en la gestión de la información, alineando los controles con los estándares actuales y agregando lineamientos para el uso seguro de servicios en la nube. Se amplían los roles y responsabilidades en la gobernanza, detallando

		funciones del Comité Institucional, el Oficial de Seguridad de la Información y la Subgerencia TIC, mientras que la Oficina de Control Interno Disciplinario asume un papel en investigaciones de incumplimientos. La política de control de acceso se refuerza con medidas estrictas para la administración de usuarios y autenticación segura. Además, se incorporan directrices sobre el uso ético de la inteligencia artificial y se actualizan los lineamientos para asegurar la continuidad del servicio en situaciones adversas. Finalmente, la política se alinea con normativas recientes en protección de datos personales y directrices de seguridad digital del CONPES, mejorando la protección y la cultura institucional

VALIDACIÓN	NOMBRE	CARGO	FECHA
Elaboró	Juan Pablo Ceballos Maria Alejandra Suarez	Contratistas Profesionales – Subgerencia e Tecnologías de la Información y las Comunicaciones	20/05/2024
Revisó	Carlos Andrés Ballesteros	Subgerente de Tecnologías de la Información y las Comunicaciones	22/05/2024
Aprobó	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	03/07/2024