MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Cra. 10 # 28-49 – Torre A, Piso 26.
(601) 6660006
Bogotá D.C – Colombia
atencionalciudadano@agenciaatenea.gov.co
www.agenciaatenea.gov.co

CONTENIDO

OBJETIVO

Establecer las políticas específicas que regulan la seguridad de la información, ciberseguridad y protección de la privacidad en La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" a través de elementos que se deben conocer, aplicar y cumplir bajo el liderazgo de la Subgerencia de Tecnologías de la Información y las Comunicaciones.

DEFINICIONES

Las definiciones detalladas a continuación, se encuentran conforme a los términos y definiciones de la ISO 27002:2022

- Activo: cualquier cosa que tenga valor para la organización.
- Ataque: intento no autorizado exitoso o fallido de destruir, alterar, deshabilitar, obtener acceso a un activo o cualquier intento de exponer, robar o hacer uso no autorizado de un activo.
- Autenticación: Provisión de seguridad de que una característica declarada de una entidad es correcta.
- Autenticidad: propiedad de que una entidad es lo que dice ser
- Cadena de custodia: posesión demostrable, movimiento, manejo y ubicación del material desde un punto en el tiempo hasta otro.
- Evaluación de impacto de la privacidad: proceso general de identificación, análisis, evaluación, consulta, comunicación y planificación del tratamiento de posibles impactos en la privacidad con respecto al procesamiento de información de identificación personal, enmarcado dentro de la gestión de riesgos.
- Gestión de incidentes de seguridad de la información: ejercicio de un enfoque coherente y eficaz para el manejo de incidentes de seguridad de la información.
- Información confidencial: información que no está destinada a estar disponible o divulgarse a personas, entidades o procesos.
- Incidente de seguridad de la información: uno o varios eventos de seguridad de la información relacionados e identificados (3.1.14) que pueden dañar los activos de una organización (3.1.2) o comprometer sus operaciones
- No repudio: Capacidad para probar la ocurrencia de un evento o acción alegado y sus entidades de origen

- Objetivo de punto de recuperación-RPO: tiempo en el que se recuperarán los datos después de que se haya producido una interrupción.
- Objetivo de tiempo de recuperación-RTO: Período de tiempo dentro del cual se recuperarán los niveles mínimos de servicios y/o productos y los sistemas, aplicaciones o funciones de soporte después de que haya ocurrido una interrupción
- Parte interesada: persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad
- Procedimiento: forma especificada de llevar a cabo una actividad o un proceso
- Proceso: conjunto de actividades interrelacionadas o que interactúan que usa o transforma entradas para entregar un resultado
- Sistema de información: conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes.
- Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas

GENERALIDADES

- La implementación de las políticas detalladas a continuación, se realizará conforme las responsabilidades definidas en la política de seguridad y privacidad de la información.
- El presente documento debe ser aplicado por todos los colaboradores institucionales, proveedores o terceros que tengan vinculo contractual con la Agencia.
- La actualización del documento se realizará conforme se identifique la necesidad.
- La continuidad de los servicios tecnológicos estará a cargo de la Subgerencia de Tecnologías de la Información y las Comunicaciones y el plan de continuidad del negocio de quien designe la alta dirección.

METODOLOGIA

A continuación, se relacionan las políticas que se deben aplicar como parte integral de la implementación del Sistema de Seguridad de la Información y cumplimiento de la Política General de Seguridad y Privacidad de la Información

Políticas organizacionales

Política de estructura organizacional de seguridad de la información

- La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea", en cumplimiento al compromiso de implementar el Sistema de Gestión de Seguridad de la Información - SGSI, establece un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información a través de su Política de seguridad y privacidad de la información.
- A través de un acto administrativo de carácter general se adoptará la estrategia de seguridad digital, identificando el alcance y responsable de su implementación.
- Las políticas que componen el sistema de Gestión de Seguridad de la Información deben ser aprobadas por la Alta Dirección o quien este designe, publicadas, comunicadas y reconocidas por los colaboradores y las partes interesadas, las actualizaciones serán a intervalos planificados o si ocurren cambios significativos.

Política de gestión de activos de Información

- Documentar un procedimiento formal para la gestión de activos de información
- Las áreas de la Agencia deben identificar y mantener actualizados los activos de información que tengan a cargo.
- Los activos de información serán responsabilidad de los lideres de cada área.
- Es responsabilidad de cada área informar las novedades que puedan afectar la integridad, disponibilidad o confidencialidad de los activos de información.
- Los activos de información son propiedad de la Agencia, por tal motivo, los colaboradores al finalizar su contrato o acuerdo deberán devolverlos.
- Se debe identificar y documentar todos los activos que deben ser devueltos, como, por ejemplo: información física, hardware de autenticación, equipos y dispositivos tecnológicos.

Política de uso de los activos

- La Entidad implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones.
- La asignación de los activos de información es para uso exclusivo del desarrollo de las actividades contractuales que le sean asignadas en la Agencia.

- El usuario de los recursos tecnológicos proporcionados por la Agencia se debe comprometer a dar buen uso, de acuerdo con las políticas definidas por el SGSI.
- Todos los colaboradores que hagan uso de los activos de información de la Agencia tienen la responsabilidad de seguir las políticas establecidas para el uso aceptable de los activos de información, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la disponibilidad de los servicios tecnológicos institucionales.

Política de uso de los recursos tecnológicos.

- Todos los colaboradores deben hacer buen uso de los activos de información a los cuales tienen acceso y que son propiedad de la Agencia, de igual forma, son responsables de cualquier uso que se les dé.
- Solo se permite manipular, destapar y actualizar los equipos de cómputo por el personal autorizado en la Subgerencia de Tecnologías de la Información y las Comunicaciones
- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, fotos o cualquier tipo de archivo que no sean de carácter institucional.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.
- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, debe ser informada de inmediato a la Subgerencia de Gestión Administrativa.
- El traslado de los recursos tecnológicos físicos se realizará a través de la Subgerencia de Gestión Administrativa y la configuración estará a cargo de la Subgerencia de Tecnologías de la Información y las Comunicaciones.
- Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información debe ser reportado a la Subgerencia de Tecnologías de la Información y las Comunicaciones en la mayor brevedad posible.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones es la única área autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
- Los equipos deben quedar apagados cada vez que el colaborador no se encuentre en la Agencia y no requiera realizar actividades vía remota.
- Definir y documentar la gestión de cambios en las instalaciones de procesamiento de información y los sistemas de información.

Política de uso del correo electrónico

- El correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los colaboradores de la Agencia.
- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Agencia.
- En cumplimiento de la iniciativa del uso aceptable del papel y la Eficiencia Administrativa, se debe optar por el uso del correo electrónico al envío de documentos físicos, siempre que las disposiciones legales lo permitan.
- Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.), en tal caso se funda la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.
- No se permite el uso de correos masivos tanto internos como externos, salvo a través de las cuentas autorizadas para tal fin.
- Todo mensaje SOSPECHOSO, SPAM o CADENA debe ser inmediatamente reportado a la Subgerencia de Tecnologías de la Información y las Comunicaciones como incidente de seguridad de la información según procedimiento establecido. No está permitido el envío y/o reenvío de mensajes en cadena, debido a que puede ser contentivo de virus, en especial si contiene archivos adjuntos con extensiones.exe, bat, prg, .bak, .pif, tengan explícitas referencias no relacionadas con la misión de la Entidad (como, por ejemplo: contenidos eróticos, alusiones a personajes famosos).
- La cuenta de correo institucional no debe ser registrada en páginas o sitios publicitarios, de comercio electrónico, deportivos, casinos, o a cualquier otra ajena a los fines institucionales.
- No se permite el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- No se dará uso del correo electrónico institucional para distribuir información institucional de carácter reservado o clasificado, sin el previo análisis y autorización del líder del área.
- El envío de mensajes desde el correo electrónico debe contener una leyenda de confidencialidad y aplicarse en la firma institucional de todos los usuarios de la Agencia.
- El único servicio de correo electrónico autorizado para el manejo de la información institucional en la Entidad es el asignado por la Subgerencia de Tecnologías de la

Información y las Comunicaciones, y que cuenta con el dominio @atenea.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad.

Política de uso de internet

- La Entidad permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones autorizará los cambios solicitados de permisos de navegación a los usuarios de La Agencia, previa solicitud del jefe de cada una de las dependencias.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones implementará herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales así mismo controla el acceso a la información contenida en portales de almacenamiento en el internet para prevenir la fuga de información.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones implementará los controles necesarios para evitar el acceso a redes sociales, sistemas de mensajería instantánea, páginas con contenido ofensivo, insultante, injurioso y violatorio de los derechos de autor; así como el acceso a sistemas de almacenamiento en la nube y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud con la respectiva justificación a La Subgerencia de Tecnologías de la Información y las Comunicaciones, para que sea evaluado y autorizado según corresponda.
- La Agencia se reserva el derecho de monitorear los accesos, y por tanto el uso del servicio de internet de todos los colaboradores, además de limitar el acceso a determinadas páginas de Internet, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad.

Política para uso de dispositivos móviles

- Todo dispositivo móvil que ingrese o se retire de la Agencia deberá ser registrado por el personal encargado de la seguridad física, en donde se pueda identificar lo siguiente:
  - Fecha y hora de ingreso.
  - Fecha y hora de salida.
  - Identificación y nombre de la persona que ingresa o retira el elemento
  - Área a la que se dirige
  - Descripción del dispositivo (serial y marca)

- Los dispositivos móviles que sean asignados en la Agencia deberán mantener la configuración respectiva para restringir la instalación de software, así como un mecanismo que impida el robo o perdida dentro de las instalaciones de la Entidad.
- Los dispositivos móviles deben estar configurados para acceder a través de credenciales de acuerdo con la asignación.
- Los dispositivos móviles de la Agencia que sean retirados de las instalaciones deben contener mecanismo de cifrado de tal forma que evite divulgación de información en caso de pérdida o robo.
- Todos los dispositivos móviles asignados deben tener instalado el antivirus institucional.
- El uso de conexión a la red para los dispositivos móviles ajenos a la Agencia deberá estar segmentada para proveer únicamente el servicio de internet, restringiendo el acceso a la data y navegación interna.

Política de uso de mensajería instantánea y redes sociales

La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" define las pautas generales para asegurar una adecuada protección de la información, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

- La información que se publique o divulgue por cualquier medio de Internet, de cualquier colaborador de la Agencia, que sea creado a nombre personal en redes sociales como -pero sin limitarse: Twitter®, Facebook®, YouTube®, blogs, Instagram, se considera fuera del alcance del Sistema de Gestión de Seguridad de la Información y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que lo genere.
- Toda información distribuida en las redes sociales que sea originada por la entidad debe ser autorizada por los lideres del área para ser socializadas.
- No se debe utilizar el nombre de la Agencia en redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la Entidad.
- Las personas designadas para el manejo y gestión de contenido en las redes sociales de la Agencia deben acatar las directrices dadas en el presente documento.
- El área que requiera la apertura de una red social bajo el dominio de la Agencia debe presentar una solicitud motivada, relacionando la necesidad, objeto y alcance de la

cuenta institucional, enunciando los datos personales de los colaboradores que realizaran la administración de la red social.

- Los responsables de cada red social deberán aplicar complejidad en las contraseñas de las cuentas institucionales, acatando los protocolos de seguridad de estas y realizando el cambio periódicamente.
- El Sistema de Gestión de Seguridad de la Información realizará la verificación de las medidas y controles implementados de seguridad, encaminadas a evitar el acceso abusivo a la plataforma, que puedan afectar la imagen y la credibilidad de la entidad.
- No se deben vincular cuentas de correo electrónico personales en las redes sociales que se apertura bajo el dominio de la Agencia.
- No se recomienda la administración de las redes sociales la Agencia en dispositivos móviles personales

Política de clasificación de la información

La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" consiente de aplicar el nivel de protección apropiado de acuerdo con el tipo de calificación establecido por las disposiciones legales, define lo siguiente:

- Las categorías de calificación de la información que se adoptaran son: INFORMACIÓN PÚBLICA, INFORMACIÓN PÚBLICA RESERVADA e INFORMACIÓN PÚBLICA CLASIFICADA.
- Todos los activos de información indiferente de su medio de almacenamiento deben ser clasificados de acuerdo con los lineamientos institucionales creados para tal fin. Esta actividad debe ser realizada por los responsables sobre la gestión de los activos.
- Toda la documentación o información generada en la Agencia debe contener clasificación.
- Desarrollar e implementar los lineamientos para el etiquetado de la información de acuerdo con las categorías definidas y adoptadas, las cuales permitirán reconocer fácilmente la clasificación del activo de información.
- La información que se intercambie en cumplimiento de acuerdos institucionales con otras entidades debe incluir la clasificación e informar al destinatario la interpretación de la clasificación con el fin de que este le asigne las protecciones requeridas.
- En el caso de los sistemas de información que contienen información sensible o crítica se deben implementar mecanismos que indiquen la clasificación e identificación del contenido.

Política para la transferencia de información

- Proteger la información transferida al interior y exterior de La Agencia.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones, realiza el control del uso de sistemas de transferencia de archivos vía FTP a terceros.
- Los canales de red usados para la transferencia de información deberán contar con un mecanismo que no permita la fuga o interceptación de información, en su defecto la información que viaja por estos deberá estar cifrada.
- Las transferencias de información deben estar amparadas por acuerdos interinstitucionales o de confidencialidad que permitan mantener los estándares de seguridad sobre esta.

Política de control y gestión de acceso

- La Subgerencia de Tecnologías de la Información y las Comunicaciones establecerá los lineamientos para la gestión de usuarios dónde se detalle el uso de credenciales únicas, así mismo, para el uso de identificaciones compartidas o grupales por razones justificadas, establecer los tiempos de bloqueo o modificación de cuentas por inactividad, intentos fallidos, cambio de roles o retiro.
- Se debe mantener un registro centralizado de los accesos suministrados.
- Los accesos se deben realizar por las herramientas autorizadas, no se permiten el uso de software de acceso remoto no licenciado por la Agencia.
- Todo aplicativo informático o software debe ser comprado o aprobado por Subgerencia de Tecnologías de la Información y las Comunicaciones.
- El control de acceso a la Información se realiza aplicando el principio de mínimo privilegio necesario para la realización de las actividades asignadas.
- El acceso a la información se realiza de acuerdo con los niveles de calificación de la información y perfil asignado al usuario.
- Para el acceso a los espacios de archivo tanto en las dependencias como el Archivo Central, se debe dar aplicación a los controles y lineamientos establecidos por la subgerencia encargada.
- Los colaboradores que, tengan bajo su responsabilidad la custodia de información física almacenada en los archivadores que se encuentra en las oficinas, deben mantener el control de acceso a esta información; por lo tanto, debe estar bajo llave. Se recomienda que las llaves se guarden en un sitio seguro, dando cumplimiento a lo establecido en la presente política.
- Los accesos con privilegios especiales deben contar con la aprobación de la Subgerencia de Tecnologías de la Información y las Comunicaciones y estar debidamente justificados por el solicitante.

- Los responsables del manejo de usuarios privilegiados deben aceptar su responsabilidad frente al uso del usuario asignado.
- Los administradores funcionales de los sistemas de información deben realizar revisiones periódicas por lo menos una semestral de los usuarios activos en los diferentes sistemas de información, dominio y red.
- Es responsabilidad de los lideres de cada área, notificar a los administradores de TI la desvinculación de un funcionario, cesiones y terminaciones anticipadas del contratista para que sean retirados los accesos de todos los sistemas incluidos los accesos físicos a las diferentes instalaciones de la Agencia.
- En el caso de los contratistas se debe realizar la configuración automática para que el día de la terminación del contrato sean inhabilitadas las credenciales asignadas.
- La agencia se reserva el uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD,

Política de establecimiento, uso y protección de claves de acceso

- Ningún usuario deberá acceder a la red o a los servicios de La Agencia, utilizando una cuenta de usuario o credenciales de otro usuario.
- Toda acción realizada usando la clave de acceso es responsabilidad directa del usuario al que se le asignó las credenciales.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.
- El cambio de contraseña solo debe ser solicitado por el titular de la cuenta, comunicándose a la Subgerencia de Tecnologías de la Información y las Comunicaciones, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato (previa autorización por parte de la Subgerencia de Tecnologías de la Información y las Comunicaciones).
- Los colaboradores propenderán por no dejar visibles las credenciales asignadas.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones Implementará mecanismos para que los usuarios cambien su contraseña de acceso al usarla por primera vez en los sistemas de información o servicios a los que se les permita el acceso; así como implementar una política de red que solicite cambio de credenciales en periodos definidos.
- Las claves o contraseñas de acceso deben contener los siguientes requisitos de seguridad:

- Tener mínimo ocho (8) caracteres alfanuméricos.
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas doce anteriores.
- La contraseña debe ser cambiada cada sesenta (60) días.
- No debe contener el nombre de usuario y caracteres consecutivos como - abcd,123456

Manejo de contraseñas para administradores de TI

- Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.
- Las contraseñas referentes a las cuentas "predefinidas" incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.
- Los administradores de TI pertenecientes a la Subgerencia de Tecnologías de la Información y las Comunicaciones no deben dar a conocer sus credenciales institucionales de acceso a los sistemas de información a terceros, sin previa autorización escrita del Subgerente de Tecnologías de la Información y las Comunicaciones.
- Los Administradores de TI pertenecientes a la Subgerencia de Tecnologías de la Información y las Comunicaciones deben emplear obligatoriamente contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación que posee la entidad de acuerdo con el rol asignado.

Política en la relación con proveedores

- Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.
- Se deben establecer obligaciones dentro de los contratos con terceros que contemplen aplicación de estándares y mejores prácticas de gestión de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad
- Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de

la información de La Agencia, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

- En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.
- Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por La Agencia.
- Los funcionarios de La Agencia que tengan responsabilidad como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.
- Todo proveedor y/o contratistas debe estar informado de las políticas y lineamientos que componen el Sistema de Gestión de Seguridad de la Información -SGSI.
- Todo proveedor y/o contratistas debe realizar la devolución de los activos de información asignados por la Agencia.
- Se deben establecer mecanismos o condiciones con los contratistas o proveedores que permitan realizar la gestión de cambios en los servicios suministrados.

Política para el uso de servicios en la nube

- En el uso de servicios en la nube contratados por la Agencia se deben gestionar los riesgos de seguridad.
- Identificar y definir la responsabilidad compartida de la seguridad de la información y los esfuerzos de colaboración entre el proveedor del servicio y la Agencia. En caso de que los acuerdos de servicios estén predefinidos y no están abiertos a negociación la Agencia debe revisar los definidos y validar que se contemplen los requisitos de confidencialidad, integridad, disponibilidad y manejo de la información de la entidad.
- La Agencia, actuando como cliente del servicio en la nube definirá si debe exigir al proveedor de servicio que se notifique antes de realizar cambios sustanciales que afecten la entidad, como los relacionados a continuación, pero sin limitarse:
  - Cambios de hardware o software, reconfiguraciones y demás que afecten o cambien la oferta de servicios en la nube.
  - Realizar tratamiento de información en una nueva jurisdicción geográfica o legal.
  - Uso de proveedores de servicios similares o subcontratados.

Política de gestión de los incidentes de la seguridad de la información

- Garantizar que los eventos e incidentes de seguridad que se presenten con los activos de información sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.
- Establecer los respondientes para la atención de incidentes dentro de la Agencia.
- Identificar y documentar contacto con autoridades, grupos de interés que manejen cuestiones relacionados con seguridad de la información e incidentes.
- Asegurar una gestión consistente y eficaz de la evidencia relacionada con incidentes de seguridad de la información para efectos de acciones disciplinarias y legales.
- Fortalecer y mejorar los controles de seguridad de la información a través de la documentación y conocimiento de los incidentes de seguridad que se presenten en la entidad.

Política de seguridad de la información durante la interrupción

- Se debe definir el conjunto de procedimientos y estrategias para contrarrestar las interrupciones en las actividades misionales de la entidad, proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.
- Prevenir interrupciones en las actividades de la plataforma informática de la Agencia que, van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.
- Los proveedores de servicios TI críticos deberán contar con planes de continuidad.
- Se debe desarrollar e implementar un Plan de Continuidad TI para asegurar que los procesos misionales de TI de la Agencia los cuales serán restaurados dentro de escalas de tiempo razonables. El plan de acción que permitirá mantener la continuidad se desarrollará teniendo en cuenta los siguientes aspectos:
  - Identificación y asignación de prioridades a los procesos críticos de TI de la Agencia de acuerdo con su impacto en el cumplimiento de la misión de la entidad.
  - Documentación de la estrategia de continuidad TI.
  - Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
  - Plan de pruebas de la estrategia de continuidad de los servicios de TI.

- Los requisitos de seguridad de la información deben incluirse en los procesos de gestión de la continuidad del negocio.

Política de cumplimiento de requisitos legales, estatutarios, reglamentarios y contractuales

- La entidad debe gestionar riesgos para prevenir el incumplimiento de obligaciones legales relacionadas con seguridad de la información.
- Todos los sistemas de información que capturen datos personales deben cumplir con la política de protección de datos personales definida por la Agencia.
- Se debe identificar, documentar y actualizar los requisitos legales y reglamentados relacionados con seguridad de la información.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones deberá garantizar que todo el software que se ejecute esté protegido por derechos de autor y requiera licencia de uso o software de libre distribución y uso.
- Mantener prueba y evidencia de propiedad del licenciamiento adquirido.
- Los colaboradores de la Agencia deben cumplir con las Leyes de derechos de autor y acuerdos de licenciamiento de software, se recuerda que es ilegal duplicar software y documentación sin la autorización del propietario bajo los principios de derechos de autor y, la reproducción no autorizada es una violación a la Ley.

Política de tratamiento de datos personales

En cualquiera sea el caso el tratamiento de datos personales se realizará conforme la Ley 1581 de 2012, sus Decretos reglamentarios y la Política de Tratamiento de Datos Personales

Datos de menores de edad: El tratamiento de los datos personales de menores de edad es facultativo y debe realizarse con autorización de los padres de familia o representantes legales del menor, en concordancia con lo establecido por la Ley 1098 de 2006 “Código de Infancia y Adolescencia” y la Política de Tratamiento de Datos Personales.

Datos personales y biométricos: En la(s) sede(s) de la Agencia en donde se realice recolección de datos personales y datos biométricos -como huellas e imágenes, se deben fijar avisos/habladores, con el fin que los titulares registrados en la Entidad conozcan sus derechos.

Sesiones virtuales: Se debe informar los asistentes que se va a realizar la grabación de esta, de tal forma que si algún asistente no está de acuerdo lo debe indicar al organizador; si no se recibe alguna observación, se da por entendido que ha dado su aprobación

Política de revisión independiente de la seguridad de la información.

- Garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo con las políticas y procedimientos implementados en la Agencia.

- A través de la Oficina de Control Interno de Gestión se realizarán las verificaciones del cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la Información.
- Todos los líderes de proceso deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su área de responsabilidad.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones a través del Sistema de Gestión de Seguridad de la Información realizará revisiones esporádicas no programadas con el fin verificar el cumplimiento de las políticas de seguridad de la información en las instalaciones de la Agencia.

Política de cumplimiento

- Los diferentes aspectos contemplados en esta Política son de obligatorio cumplimiento para todos los colaboradores de la Agencia. En caso de que se infrinjan las políticas de seguridad de forma intencional o por desconocimiento, la Agencia tomará las acciones disciplinarias y legales correspondientes.
- Con la aplicabilidad de las políticas establecidas se debe prevenir el incumplimiento de las leyes, estatutos, regulaciones y obligaciones contractuales que se relacionen con los controles de seguridad.

Política de seguridad del recurso humano

- Se debe asegurar que los funcionarios, contratistas y demás colaboradores de La Agencia, adopten sus responsabilidades en relación con las políticas de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir los riesgos.
- Los acuerdos contractuales deben establecer la responsabilidad del colaborador en cuanto a seguridad de la información -derechos de autor, confidencialidad y no divulgación de la información durante y después del empleo.
- Establecer estrategias para que los colaboradores tomen conciencia sobre lo relacionado con seguridad de la información.
- Articular los procedimientos disciplinarios en situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información, conforme a las normas que lo reglamenten en el sector público.
- Implementar procedimientos que permitan identificar las novedades, desvinculaciones, terminaciones o cesiones de contrato, con el fin de retirar o modificar los accesos físicos y lógicos en la Agencia.

Política de trabajo a distancia

- La Subgerencia de Tecnologías de la Información y las Comunicaciones propenderá por la identificación de necesidad y licenciamiento de la VPN - Virtual Private Network
- Las actividades de acceso remoto (uso de VPN - Virtual Private Network) a los sistemas informáticos y activos de información de la Entidad, se autorizan de acuerdo con las necesidades específicas del área solicitante.
- Se recomienda que mientras se haga uso de VPN desde un equipo personal, éste tenga instalado y actualizado el antivirus y que el sistema operativo cuente con las actualizaciones de seguridad y licenciado.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones realizará las configuraciones de seguridad, aprovisionamientos y revocación de acceso a la VPN

Política de reporte de eventos de seguridad de la información

- Los colaboradores y terceros deben reportar cualquier evento sospechoso observado en los activos de información.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones definirá y socializará los canales para el reporte de eventos de seguridad detectados.

Política de seguridad física

Política de perímetros y entrada física

- La Agencia debe implementar un sistema de seguridad física para las instalaciones de la Agencia.
- Se deben implementar alarmas de detección de intrusos a los centros de datos y centros de cableado de la Agencia.
- Definir y usar perímetros de seguridad para proteger las áreas de procesamiento de información sensible o critica, teniendo en cuenta:
  - Todas las puertas externas deberán tener mecanismos de control que eviten el acceso no autorizado.
  - Las puertas y ventanas se deben mantener cerradas con llave cuando no hay supervisión.
  - Prohibir el uso de equipo fotográfico, de video, audio u otro equipo de grabación cuando no se cuente con autorización para ello.
  - Los visitantes deben registrarse en la entrada, ser autorizados por un colaborador para ingresar y durante su estancia deben estar acompañados por el funcionario o contratista con el cual están desarrollando su actividad.

- Los controles de acceso físico a las instalaciones deben permitir el acceso únicamente al personal autorizado.
- Todos los colaboradores deben portar el carné en lugar visible, en caso de ser visitante se debe portar una escarapela que lo identifique, se debe notificar al personal de vigilancia cualquier caso de visitantes solos y sin identificación visible.
- Para el caso de las áreas de despacho y carga se debe:
  - Inspeccionar el material que ingresar para detectar presencia de materiales peligrosos.
  - Restringir para el personal identificado y autorizado

Política de escritorio despejado y pantalla limpia

- Los colaboradores y terceros que tienen algún vínculo con La Agencia deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- Todos los equipos y sistemas de información deben configurarse con una función de tiempo de espera o cierre de sesión automático.
- Los usuarios de los sistemas de información y comunicaciones de la Agencia deben bloquear la pantalla de su computador, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
- Los usuarios de los sistemas de información deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.
- Al imprimir documentos con información pública reservada y/o pública clasificada, deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

Política de protección contra amenazas físicas y ambientales

- Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.
- En las instalaciones del centro de datos o de los centros de cableado, No está permitido:
  - Fumar dentro de las instalaciones.
  - Introducir alimentos o bebidas.
  - El porte de armas de fuego, corto punzantes o similares.
  - Mover, desconectar y/o conectar equipo de cómputo sin autorización.
  - Modificar la configuración del equipo o intentarlo sin autorización.

- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los recursos tecnológicos o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los recursos tecnológicos.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

- Contar con herramientas que permitan registrar el acceso de los colaboradores a estas áreas.
- Revisar y actualizar periódicamente los derechos de acceso.
- Cada Gabinete o armario contiene llave de ingreso y/o tarjeta de acceso, las cuales deben permanecer custodiadas por el colaborador designado para tal fin.
- Considerar la implementación de controles contra incendios, inundaciones, sobretensiones eléctricas y en general de las posibles amenazas físicas y ambientales.
- Los medios y equipos donde se almacena procesan o comunica la información (física o electrónica), deben mantenerse con las medidas de protección físicas y lógicas.

Política de medios de almacenamiento

- Los medios de almacenamiento extraíble pueden ocasionalmente generar riesgos para la Agencia al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada.
- Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través de la Subgerencia de Tecnologías de la Información y las Comunicaciones y será objeto de auditorías de seguridad mediante las herramientas consideradas para tal fin.
- Solo se habilitarán los puertos de conexión de medios de almacenamiento extraíbles si existe una razón institucional para su uso.
- Se debe realizar monitoreo a la transferencia de información cuando sea necesario utilizar medios de almacenamiento extraíble.
- Se debe implementar un procedimiento para la transferencia de medios físicos, se entenderán todos los activos de información físicos.

Política de seguridad del cableado

- Se debe implementar controles que permitan proteger las líneas eléctricas y de telecomunicaciones de cortes accidentales.
- Los cables de alimentación y comunicación deben estar separados para evitar interferencias.
- Implementar conductos blindados, cajas cerradas y alarmas en los puntos de terminación.
- Establecer mecanismos de acceso controlado a los paneles de conexión y centros de cableado.
- Se debe propender por el uso de cables de fibra óptica.

Política de mantenimiento de equipos

- Se debe establecer un cronograma para el mantenimiento de los equipos tecnológicos (UPS, routers, computadores, aires, Switch)
- Solo las personas autorizadas realizaran las reparaciones y mantenimientos respectivos.
- Cada mantenimiento debe contar con una ficha técnica que permita establecer el mantenimiento realizado, fecha, reparaciones, persona que realiza la actividad y quien recibe a satisfacción.
- En caso de ser requerido un mantenimiento remoto, se solicitará la autorización de La Subgerencia de Tecnologías de la Información y las comunicaciones a través de un mecanismo seguro y licenciado por la Entidad.

Política de eliminación segura o reutilización de equipos

- En los casos en que se almacene información en equipos que se encuentran en las salas de reuniones de la Entidad, salas de juntas y salones de capacitación; las personas que han realizado la reunión, en el momento que no se requiera su uso en estos dispositivos, deben eliminarla de forma permanente; con el fin de evitar que personas no autorizadas puedan conocerla.
- Cuando no se requiera la información contenida en un medio de almacenamiento reusable, se debe borrar para que no sea recuperable y registrar los resultados como prueba de la eliminación. En caso de los equipos en condición de alquiler, se debe realizar el borrado antes de la devolución.
- La información almacenada con nivel alto de confidencialidad o integridad en medios removibles debe contar con técnicas de cifrado para evitar accesos no autorizados.
- Para los medios que contienen información confidencial, se deben almacenar y disponer de forma segura, mediante incineración, destrucción a través de máquinas

destinadas para tal fin o proceso de borrado seguro, de acuerdo con las directrices de la Subgerencia de Gestión Administrativa y la Subgerencia de Tecnologías de la Información y las comunicaciones.

- En cualquiera sea el caso de realizar destrucción de algún componente tecnológico, se ejecutará bajo los lineamientos del Sistema de Gestión Ambiental.

Política de las operaciones TIC
Política de dispositivos tecnológicos y redundancias

- Definir y documentar las actividades operaciones especificando los lineamientos para:
  - Copias de respaldo
  - Reinicio y recuperación del sistema en caso de falla
  - Manejo de errores y otras condiciones.
  - Contactos de soporte en caso de dificultades técnicas inesperadas.
- Realizar seguimiento al uso de recursos y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema, considerando documentar planes de gestión de capacidad para los sistemas críticos de la misionalidad.
- Los servicios y dispositivos tecnológicos deben estar monitoreados en cuanto a: seguimiento de intentos de accesos fallidos y compartimientos anómalos.
- Los Colaboradores no deben instalar ningún tipo de canal de transmisión, módems, ni cambiar la configuración de sus equipos sin la previa aprobación de la Subgerencia de Tecnologías de la Información y las Comunicaciones.
- Los colaboradores no tienen permitido descargar, utilizar e instalar software externo en los recursos tecnológicos institucionales a menos que sea aprobado e instalado por la Subgerencia de Tecnologías de la Información y las Comunicaciones.
- Implementar controles de detección, prevención y recuperación para proteger los activos de información contra ataques de código malicioso.
- La asignación de dispositivos tecnológicos deberá realizarse a través de registro y entregar con las configuraciones de: dominio, cifrado de disco, restricción de instalación de software, protección contra malware, des habilitación para borrado, bloqueo remoto, partición del disco duro y demás consideradas en las políticas anteriores.
- la Subgerencia de Tecnologías de la Información y las Comunicaciones propenderá por:

- Licenciar software de protección contra código malicioso en todos sus servidores, equipos de cómputo y los archivos intercambiados por correo electrónico tanto entrantes como salientes.
- Establecer mecanismos para mantener actualizados todos los sistemas de procesamiento de información (parches de software y actualizaciones).

- Identificar los servicios tecnológicos más críticos y considerar la implementación de redundancias necesarias para garantizar la continuidad del servicio.

Política de accesos con privilegios.

- La asignación de los accesos con privilegios debe controlarse a través de un proceso.
- Las solicitudes deben ser realizadas y aprobadas por el responsable del activo de información.
- Los accesos con privilegios deben estar limitadas por un rango de tiempo específico.
- Revisar regularmente los accesos con privilegios otorgados.
- Se debe tener en cuenta que los accesos con privilegios son para realizar tareas administrativas dentro de los componentes tecnológicos y en ningún momento para realizar actividades de uso común del usuario.
- Los accesos con privilegios deben estar asociados a un usuario especifico, si la cuenta contiene una identificación genérica no se debe hacer uso por varios administradores.

Política de acceso a sistemas y aplicaciones

- El acceso a la información y a las funcionalidades de las aplicaciones se debe restringir, de acuerdo, con los niveles de autorización para cada usuario o grupo de usuarios.
- Los sistemas y aplicaciones deben mantenerse monitoreados y auditados.
- Las credenciales para acceder a los ambientes de pruebas y producción se deben diferenciar de forma que permitan identificar cada usuario para cada ambiente.
- Se debe controlar el acceso a códigos fuente de programas y elementos asociados (diseños, especificaciones, planes de prueba, resultados), para evitar la introducción de funcionalidades no autorizadas o cambios involuntarios, así mismo, para mantener la confidencialidad de la propiedad intelectual, por tal motivo:
  - Las librerías de programas fuente, no deberían estar contenidas en los ambientes de producción.
  - Establecer un repositorio formal para el almacenamiento.
  - Controlar los cambios para el mantenimiento y copia de las librerías de fuentes de programas.

- Mantener un registro de auditoría de todos los accesos

- Se debe mantener los siguientes componentes, pero sin limitarse;
  - Validar las credenciales de acceso al completar todos los datos de entrada, en caso de error el sistema no deberá informar cual es el dato correcto o incorrecto.
  - Proteger contra intentos de ingreso mediante ataques de fuerza bruta.
  - Mantener registro de intentos exitosos y fallidos de acceso.
  - No mantener visible la contraseña que se está ingresando.
  - No transmitir contraseñas en texto claro en las redes o medios de comunicación.
  - No dar la opción al usuario de recordar las credenciales
  - Datos de acceso (fecha y hora de inicio de sesión exitoso)
  - Finalizar las sesiones inactivas después de un periodo de inactividad de tiempo, con especial rigurosidad para lugares públicos, externos o dispositivos móviles.
  - Bloqueo de credenciales tras 3 intentos máximos erróneos.
  - Bloqueo de los equipos de cómputo tras 5 minutos de inactividad.

Política de gestión de vulnerabilidades

- Identificar y definir las estrategias de monitoreo de vulnerabilidades técnicas.
- Se debe exigir a los proveedores de servicios tecnológicos la notificación y plan de remediación de vulnerabilidades
- Realizar pruebas planificadas y documentadas para evaluar vulnerabilidades.
- Validar riesgos del despliegue de actualizaciones de firmware o sistemas operativos antes de su instalación

Política de controles criptográficos

- Implementar controles para proteger activos de información reservados, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.
- La Agencia no establece un lineamiento de ciclo de vida de llaves criptográficas, toda vez que, la asignación de la clave para el cifrado de la información en la herramienta, la establece el usuario que genera o administra la información a cifrar, teniendo siempre presente que, en caso de olvidar la clave, la información cifrada no es recuperable.
- Se debe contar con herramientas que permitan el cifrado de información en medios de almacenamiento.
- Se debe instalar y configurar herramientas de cifrado de información en los portátiles de la Agencia.

Política de respaldo y restauración de información

- Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.
- Los administradores de la plataforma que realiza las copias de seguridad verificarán la correcta ejecución de los procesos de backup.
- Los administradores de la plataforma de copias de respaldo (backup) de la entidad, mensualmente deben generar tareas de restauración aleatorias de la información de las bases de datos definidas por la Subgerencia de Tecnologías de la Información y las Comunicaciones, quedando registradas en el formato definido para tal fin; estas restauraciones deben ser documentadas, con el fin de garantizar la continuidad de las actividades realizadas en la Agencia, usando las herramientas tecnológicas en caso de presentarse la no disponibilidad de la información almacenada en las bases de datos.
- Es responsabilidad de los colaboradores almacenar la información en los medios dispuestos por la Subgerencia de Tecnologías de la Información y las Comunicaciones, con el fin de generar las copias en las unidades correspondientes.
- Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información.
- Teniendo en cuenta que, la información generada, producida y tratada por el colaborador es producto de la ejecución de actividades institucionales no se entregaran copias de respaldo de la información contenida en correos electrónicos, sistemas de información, estaciones de trabajo y unidades de almacenamiento.
- Mantener custodiadas copias idénticas de sistemas operativos que respondan a eventos de contingencia y disminuyan el impacto en caso de falla irreversible.

Política de seguridad de las comunicaciones

- Implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento de la Agencia.
- Segmentar los servicios de información, usuarios y sistemas, controlando así el tráfico.
- Los servicios de red deben estar protegidos a través de medios de autenticación.
- Implementar los mecanismos técnicos requeridos para la conexión segura con los servicios de red.
- Disponer de zona DMZ entre la red interna y externa con el objetivo limitar conexiones desde la red interna hacia Internet y conexiones desde internet hacia la red interna.
- Se debe disponer de servicio de internet para visitantes de la entidad.

Política de registro y seguimiento de eventos de sistemas de información y comunicaciones

- Identificar los sistemas críticos de la Agencia y documentar una metodología de revisión y escritura de eventos (Event Logs), que permita identificar las actividades por usuario, excepciones, fallas y eventos de seguridad que no den espacio a la alteración, uso no autorizado o repudio, en caso de presentarse materialización del riesgo y ser utilizados como medio probatorio.
- Mantener los relojes de todos los dispositivos tecnológicos con una única fuente de referencia, esto con el fin de mantener la exactitud del tiempo y permita correlacionar los eventos y logs.

Política de adquisición, desarrollo y mantenimiento de sistemas de información

- Garantizar que la seguridad es parte integral del ciclo de vida de los sistemas de información.
- Documentar lineamiento de control de instalación y cambios de los sistemas, para mantener operativas las aplicaciones basadas en estos y que permitan procedimientos de retroceso (RollBack) exitosos.
- Definir y documentar los requisitos de seguridad para la adquisición, desarrollo de los sistemas y mejoras de los existentes.
- Se debe aplicar mecanismos de auditoría a todos los sistemas de información y se evaluara su tiempo de retención teniendo en cuenta la capacidad de almacenamiento institucional, en todo caso, este no debe ser inferior a 3 meses.
- Garantizar la separación de los entornos de desarrollo, pruebas y producción de los sistemas de información.
- Definir y documentar los entornos para el almacenamiento de los códigos y sus versiones.
- Ejecutar revisiones periódicas al licenciamiento de software y desinstalar de los equipos de cómputo, el software que no se encuentre licenciado.
- Establecer y documentar las prácticas seguras, criterios de solicitud y pruebas de calidad y aceptación sobre el desarrollo
- Las solicitudes para uso de software libre serán avaladas previo concepto del oficial de seguridad.
- Las actividades de instalación de software y actualización de los archivos de configuración del sistema solo pueden ser realizadas por personal de la Subgerencia de Tecnologías de la Información y las Comunicaciones, por tanto, está prohibido modificar, alterar o programar cualquier tipo de configuración.

- Asegurar que las bases de datos utilizadas en ambientes de prueba sobre las etapas de desarrollo de soluciones de información no corresponden a información real o la misma debe ser modificada para tales fines.
- El desarrollo de aplicativos o sistemas de información diseñado por terceros debe estar bajo estándares de desarrollo de la Subgerencia de Tecnologías de la Información y las Comunicaciones y alineado a las políticas de seguridad de la información.
- Los datos de prueba no deben contener datos personales o información sensible, de ser necesario este contenido se deben utilizar mecanismos de enmascaramiento o sustitución de datos.

Política de protección de la información durante auditorias
Cuando se considere realizar auditorías a los sistemas de información y demás componentes de almacenamiento de esta, se debe tener en cuenta lo siguiente:

- La auditoría debe contemplar de manera específica el sistema al cual requiere acceso.
- Los accesos solo serán autorizados en modo lectura.
- Si se requiere un acceso diferente al modo lectura, se otorgará para copias aisladas del sistema con todos los parámetros de seguimiento de seguridad -logs.
- Si las pruebas afectan la disponibilidad estas deben realizarse fuera del horario laboral.

DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad (Statement of Applicability - SOA), es un documento que lista los controles que se van a implementar en la Agencia, así como las justificaciones de aquellos controles que no serán implementados.

Para el caso específico de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea", este tipo de análisis se hace evaluando el cumplimiento de la norma ISO 27002, para cada uno de los controles establecidos en los dominios o temas relacionados con la gestión de la seguridad de la información que este estándar especifica.

TABLA DE CONTROL DE MODIFICACIONES

No. Revisión	Fecha de Cambio	Apartado modificado	Descripción
01	20/10/2022	Fechado y Codificado	Versión 01
02	16/01/2023	modificación de pie de página según manual de identidad de atenea y asignación cuadro control de cambios	Versión 02

Elaboró: María Alejandra Suárez Rojas	**Revisó:** Lira Jazmín Pineda Moreno	**Aprobó:** Mario Alfonso Pardo
Cargo: Oficial de seguridad de la información	**Cargo:** Subgerente de TIC	**Cargo:** Gerente de estrategia encargado
Fecha: 20/10/2022	**Fecha:** 20/10/2022	**Fecha:** 20/10/2022