Tabla de contenido **Pág.**

1. Introducción

La Unidad Administrativa Especial de Alimentación Escolar - Alimentos para Aprender, reconoce que la información que gestiona es uno de los activos más importantes para su funcionamiento y que ésta puede ser de naturaleza legal, estratégica, financiera, operativa y en algunos casos corresponde a datos personales de empleados públicos, contratistas y grupos de interés. Igualmente, es consciente de las amenazas que enfrenta dicho activo y de las consecuencias a las que se expone la Entidad cuando ésta no cuenta con las medidas de seguridad adecuadas.

En ese sentido, se hace necesario propender por la seguridad y privacidad de la información y seguridad digital en la Entidad, teniendo presente que la vulneración se encuentra en cualquier estado de su ciclo de vida (creación, procesamiento, almacenamiento, transmisión, uso o destrucción), puede llegar a tener impactos a nivel legal, de imagen, operacional, en el cumplimiento de la misión y los objetivos estratégicos de la Entidad.

Teniendo en cuenta lo anterior, el presente manual establece los principios orientadores de seguridad y privacidad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad y continuidad, de la información de la Entidad, así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información y seguridad digital, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI.

2. Objetivo

Establecer los lineamientos para la adecuada gestión de la seguridad, privacidad de la información y seguridad digital en el Unidad Administrativa Especial de Alimentación Escolar - Alimentos para Aprender, enmarcados en la implementación de un Sistema de Gestión de Seguridad y privacidad de la Información, basado en la identificación y valoración de los riesgos asociados, propendiendo por la protección de la confidencialidad, integridad, disponibilidad, privacidad de la información, continuidad en la operación de los servicios, y por el cumplimiento de la normatividad vigente aplicable.

3. Alcance

Los lineamientos contenidos en el presente manual aplican a la información circulante en el mapa de procesos, Tablas de Retención Documental – TRD, documentos de apoyo, infraestructura tecnológica, sistemas de información y demás información que administre, proteja y preserve la Unidad Administrativa Especial de Alimentación Escolar - Alimentos para Aprender y cualquier entidad que ejerza en su nombre a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, basados en las leyes y otras regulaciones aplicables, la norma ISO 27001:2022, las

recomendaciones del estándar ISO 27002:2022, así como las determinaciones y guías del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), para el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos.

4. Términos y definiciones

Con el objeto de precisar el alcance de los principales conceptos utilizados en este documento, se transcriben las definiciones [ISO 27000:2013]:

- **Activo de información:** es cualquier recurso (físico, lógico o humano) que pueda contener o procesar información relevante para la Entidad o el proceso en el cual es requerido.
- **Activo crítico:** son aquellos elementos o componentes que hacen parte de la infraestructura critica.
- **Administración de riesgos:** proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y deberá llevarse a cabo en forma periódica.
- **Alta dirección:** persona o grupo de personas que dirigen y controlan al más alto nivel una entidad. Es la máxima autoridad en el sistema.
- **Amenaza:** causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.
- **Análisis de impacto al negocio:** es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.
- **Autenticación:** proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Centro de cableado:** es el lugar donde se ubican los recursos de comunicación de Tecnología de información, como Switch, patch, panel, UPS, router, cableado de voz y de datos.
- **Ciberactivo:** se identifica como foco de la ciberseguridad los activos digitales como datos, dispositivos y sistemas que permiten a la organización cumplir con sus objetivos de negocio.
- **Ciberactivo crítico:** dispositivo para la operación confiable de activos críticos.
- **Ciberseguridad:** es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
- **Cifrado:** También conocida como “criptografía” es una ciencia que hace uso de métodos y herramientas matemáticas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un

algoritmo, usando para ello dos o más claves, con lo que se logra en algunos casos la confidencialidad, en otros la autenticidad, o bien ambas simultáneamente.

- **Confiabilidad de la información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad:** propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- **Control:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Control correctivo:** aquellos que permiten, después de ser detectado el evento no deseado, el restablecimiento de la actividad.
- **Control detectivo:** control que está diseñado para identificar un evento o resultado no previsto después de que se haya producido.
- **Control disuasorio:** control que reduce la posibilidad de materialización de una amenaza, por ejemplo, por medio de avisos disuasorios.
- **Control preventivo:** control que está diseñado para evitar un evento no deseado en el momento en que se produce.
- **Control de Acceso:** Para efectos de este documento, el control de acceso hace referencia a todas las acciones, mecanismos, protocolos y otras salvaguardas que como consecuencia de los resultados de los análisis de riesgos indiquen que se debe restringir tanto el número de personas (colaboradores de la entidad o personal externo), como la disponibilidad de uso de activos de información o recursos de la Entidad.
- **Código malicioso:** conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de autoreplicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.
- **Datacenter:** se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.
- **Dato personal:** es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados.
- **Dato personal público:** toda información personal que es de conocimiento libre y abierto para el público en general.
- **Dato personal privado:** toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general.

- **Dato semiprivado:** dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general. (Ej. Datos financieros, crediticios).
- **Datos sensibles:** es el dato que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos (artículo 5° Ley 1581 de 2012).
- **Desarrollo Seguro:** conjunto de buenas prácticas de trabajo, consideraciones metodológicas, definición de ambientes de trabajo e inclusión de elementos de seguridad y calidad en el desarrollo de soluciones de software, que enmarcan controles preventivos, predictivos y de auditoria tanto para el código fuente de la solución, como para los elementos tecnológicos que la soportan.
- **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.
- **Dispositivos móviles:** expresión general, usada para identificar aquellos elementos tecnológicos capaces de visualizar, procesar o intercambiar información y archivos digitales. Para efectos de este documento se consideran dispositivos móviles, los siguientes elementos: Computadora portátil, tableta de datos (Tablet), teléfono celular, teléfono celular inteligente (smartphone), cámaras fotográficas, discos duros extraíbles, Unidades de almacenamiento de datos USB, SD-Card, Micro-SD, entre otros.
- **DMZ:** sigla en inglés de DeMilitarized Zone hace referencia a un segmento de la red que se ubica entre la red interna de una organización y la red externa o internet.
- **Equipos activos de red:** son todos los dispositivos que hacen la distribución de las comunicaciones a través de la red de datos.
- **Escritorio Limpio:** Término que hace referencia a cada uno de los puestos de trabajo de los colaboradores de la Unidad que deben permanecer ordenados para evitar posibles pérdidas, uso indebido o daños de la información física a cargo de cada colaborador. Así como al escritorio electrónico de los equipos de cómputo de la Entidad.
- **Evaluación de riesgos:** es la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de esta, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad.
- **Evento:** ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede tener una o más consecuencias, o puede tener diferentes causas; puede consistir en algo no ocurrido, y puede ser referido algunas veces como un “incidente” o “accidente”.

- **Evento de seguridad de la información:** ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles, o una situación desconocida que puede ser relevante para la seguridad.
- **Gestión de incidentes de seguridad de la información:** ejercicio de un enfoque coherente y eficaz para el tratamiento de los incidentes de seguridad de la información.
- **Gestión de Llaves:** llamadas claves de protección, son los elementos físicos o lógicos que deben ser usados para poder aplicar el proceso inverso a la protección mediante cifrado. Estas llaves generalmente están asociadas a las herramientas usadas para cifrar la información y deberían ser protegidas por los responsables de la aplicación del cifrado de archivos, por sus jefes inmediatos y por los destinatarios de los activos de información que fueron protegidos con cifrado. La gestión de llaves permite a la Unidad que la información que se protege mediante cifrado quede expuesta o inutilizable por efectos de pérdida, daño o interceptación de las claves usadas durante la etapa de protección, definiendo responsabilidades y mecanismos de gestión de estas.
- **HASH:** es una función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija. Por extensión, al calcular el HASH de un archivo, se le otorga un nivel de confianza básico, para ejercer control sobre la realización de cambios o modificaciones en su contenido, puesto que cualquier modificación del contenido afecta el valor del HASH calculado originalmente.
- **Impacto:** se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Incidente de seguridad:** evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** son todos los datos relacionados que tienen significado para la Unidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades y, en consecuencia, necesita una protección adecuada.
- **Información de identificación personal (IIP):** cualquier información que se pueda utilizar para establecer un vínculo entre la información y la persona natural a la que se refiere dicha información o esté o pueda estar directa o indirectamente vinculadas a una persona natural.
- **Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Interrupción:** incidente ya sea anticipado o imprevisto, que causa una desviación negativa y no planificada de la entrega prevista de productos y servicios según los objetivos de una organización.
- **IIP principal:** persona natural a la que se refiere la información de identificación personal.
- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.

- **Medio removible:** los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son Memorias USB, Discos duros extraíbles, DVD y CD.
- **Mesa de servicios:** constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de servicios que la Subdirección de Información recolecta las necesidades que tienen las dependencias en cuanto a los recursos tecnológicos.
- **No repudio:** el emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.
- **Oficial de seguridad de la información:** es la persona que cumple la función de supervisar el cumplimiento de la Política, coordinar el Comité de Seguridad de la Información y de asesorar en la materia a los integrantes de la entidad que así lo requieran.
- **Paneles de conexión (patch panel):** elemento encargado para la organización de conexiones en la red.
- **Pantalla Limpia:** se refiere puntualmente al elemento del sistema operativo del computador, que se conoce como “escritorio”, que es la pantalla principal que se observa una vez que inicia el computador. En dicha pantalla solamente se deberían encontrar los íconos de los programas utilizados más frecuentemente.
- **Partes interesadas:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de continuidad de negocio:** actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.
- **Plan de tratamiento de riesgos:** documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma
- **Privacidad de la información:** el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias.
- **Propietario del riesgo:** persona o proceso con responsabilidad y autoridad para gestionar un riesgo.
- **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **Punto Objetivo de Recuperación – RPO:** punto en el tiempo hasta el que se recuperarán los datos después de que haya producido una interrupción.
- **Relaciones con los Proveedores:** es el aspecto de definición y documentación de los conductos regulares para reducir que deben ser cumplidos para atender los posibles incidentes asociados con la modificación NO

autorizada o NO intencional, o el uso indebido de la Información sensible que se debe intercambiar con los proveedores o terceras partes relacionadas con la Unidad.

- **Riesgo:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **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.
- **Sistema de información:** se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso de la Entidad.
- **Tecnologías de la información:** es el conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de la información.
- **Teletrabajo:** es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.
- **Terceros:** personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad. Usuarios externos al Ministerio TIC que en algún momento pueden llegar a interactuar por las tareas propias de su trabajo. Entre estos se pueden considerar a los clientes y entes de vigilancia, control y/o certificación.
- **Test de penetración:** es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.
- **Tiempo Objetivo de Recuperación – RTO:** periodo de tiempo dentro del cual los niveles mínimos de servicios o productos y los sistemas, aplicaciones o funciones de apoyo se deberían recuperar después de una interrupción.
- **Transferencia de Información:** hace referencia a documentación específica de políticas técnicas, procedimientos y controles de transferencia entre las partes, para proteger la transferencia de la información sensible mediante el uso de las tecnologías de comunicaciones aplicables entre las partes interesadas.
- **Violación de la seguridad de la información:** compromiso de seguridad de la información que conduce a la destrucción, pérdida, alteración, divulgación o acceso no deseados a, información protegida trasmitida, almacena o procesada de otro modo.
- **VPN:** de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.
- **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5. Marco normativo

La Unidad Administrativa Especial de Alimentación Escolar - Alimentos para Aprender referencia las siguientes normas y modelos para la gestión de la seguridad y privacidad de la información, y seguridad digital:

- **Constitución Política de Colombia.** Artículos 15, 20, 23 y 74.

✓ **Leyes**

- **Ley 23 de 1982.** Sobre derechos de autor
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 527 de 1999.** Por 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.
- **Ley 594 de 2000.** Por medio de la cual se expide la Ley General de Archivos.
- **Ley 850 de 2003.** Por medio de la cual se reglamentan las veedurías ciudadanas.
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1221 del 2008.** Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- **Ley 1273 de 2009.** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- **Ley 1474 de 2011.** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **Ley 1952 de 2019.** Por medio de la cual se expide el código general disciplinario.

✓ **Decretos**

- **Decreto 2609 de 2012.** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 0884 del 2012.** Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
- **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1074 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- **Decreto 1080 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- **Decreto 728 de 2017.** Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- **Decreto 1499 de 2017.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 1008 del 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 612 de 2018.** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- **Decreto 2106 de 2019.** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Decreto 620 de 2020.** Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- **Decreto 767 de 2022.** Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 338 de 2022.** Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- **Decreto 88 de 2022**. "Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los articulas 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.

✓ **Resoluciones**

- **Resolución 1519 de 2020.** Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- **Resolución 054 de 2020.** Por la cual se crea el Comité Institucional de Gestión y Desempeño de la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender, y se establecen sus funciones.
- **Resolución 0020 de 2021.** "Por la cual se adopta el Modelo Integrado de Planeación y Gestión – MIPG, en la Unidad Administrativa Especial de Alimentación Escolar - Alimentos para Aprender – Alimentos para Aprender.
- **Resolución 0500 de 2021.** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- **Resolución 746 de 2022.** Por la cual se fortalece el Modelo de Seguridad y Privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
- **Resolución 063 de 2023.** Por la cual se adopta la Política de seguridad y privacidad de la información y seguridad digital, como uno de los elementos habilitadores de la Política de Gobierno Digital.
- **Resolución 064 de 2023.** Por la cual se adopta la Política y los Procedimientos para la Protección y Tratamiento de Datos Personales de la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender
- **Resolución 304 de 2025.** Por medio de la cual se adopta el SIG en la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender.

✓ **CONPES**

- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.
- **CONPES 3995 de 2020.** Política Nacional de Confianza y Seguridad Digital.
- **CONPES 4144 de 2025.** Política Nacional de Inteligencia Artificial.

6. Desarrollo

Política General de Seguridad y Privacidad de la Información y Seguridad Digital

Los sujetos descritos en el ámbito de aplicación deberán preservar y administrar la integridad, confidencialidad, disponibilidad, privacidad, legalidad y confiablidad de la información digital y física, que se produce en el marco de la operación de sus procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a los de las normas técnicas colombianas, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, promoviendo el desarrollo, la implementación y seguimiento a la Política Pública de Alimentación Escolar.

6.1 Políticas específicas

Para el desarrollo del Sistema de gestión de seguridad y privacidad de la información y seguridad digital se han tenido en cuenta los controles de referencia especificados en la NTC-ISO-IEC 27001:2022 en su Anexo A, lo anterior, para la debida implementación, mantenimiento, operación y mejora continua de dicho Sistema.
Por esta razón se procede a formular y desarrollar dichos controles contenidos en las políticas específicas al interior de la Unidad Administrativa Especial de Alimentación Escolar – UAPA, los cuales serán objeto de seguimiento en su implementación a través del Formato MST-FR-15 Seguimiento implementación controles de seguridad y privacidad de la información.

6.1.1 Controles Organizacionales

Control SI-A.5.1 Políticas de SI

Control SI-A.5.4 Responsabilidades de gestión

La Unidad deberá a través de la Alta dirección definir, aprobar y publicar la política de seguridad y privacidad de la información y las políticas de temas específicos, además estas deben ser comunicadas y reconocidas por el personal y las partes interesadas pertinentes y revisadas a intervalos planificados y si se producen cambios significativos.

Control SI-A.5.2 Roles y responsabilidades en la SI

La Subdirección de Información a través del oficial de seguridad y privacidad de la información, definirán y asignarán los roles y responsabilidades de seguridad y privacidad de la información de acuerdo con las necesidades de la Unidad.

Control SI-A.5.3 Segregación de funciones

Los activos de información deberán estar bajo la responsabilidad del Líder del Proceso para evitar conflictos y reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de información de la Unidad.

Control SI-A.5.5 Contacto con autoridades

La Unidad en conjunto con el Oficial de seguridad y privacidad de la información, debe mantener los contactos con autoridades (Policía Nacional, INTERPOL, Bomberos, Defensa Civil, Grupos de atención de desastres, etc.) u otros especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad y privacidad de la información y seguridad digital que requiera de asesoría externa, siempre que esta sea informada por el líder del proceso afectado.

Control SI-A.5.6 Contacto con grupos de interés especial

La Unidad a través del Oficial de seguridad y privacidad de la Información y demás personal que este determine debe mantener contacto con grupos de interés especializados en seguridad y privacidad de la información y seguridad digital, con el fin de compartir e intercambiar conocimientos en pro de la mejora continua del Sistema de gestión de seguridad y privacidad de la información.

Control SI-A.5.7 Inteligencia de amenazas

La Subdirección de Información a través del Oficial de seguridad y privacidad de la información recopilará y analizará la información proveniente de diferentes fuentes relativa a las amenazas a la seguridad y privacidad de la información, que permita tomar las medidas de mitigación adecuadas ante incidentes.

Control SI-A.5.8 Seguridad de la Información en la gestión de proyectos

El asesor de Planeación, con el apoyo del Oficial de Seguridad y Privacidad de la información, deberán definir e incluir en la metodología de gestión de proyectos de la Unidad, y en todas sus fases, los aspectos relacionados con la seguridad y privacidad de la información y seguridad digital. Para este fin se tendrán en cuenta los siguientes aspectos:

- Durante la ejecución del proyecto se deben cumplir los lineamientos de la política de seguridad y privacidad de la información, seguridad digital, y continuidad de la operación de los servicios, adicionalmente la política de tratamiento de datos personales de la Unidad que apliquen al objeto del proyecto.
- Se debe realizar seguimiento y revisión periódica de los lineamientos correspondientes a seguridad y privacidad de la información y seguridad digital enmarcado en la normativa interna de la Unidad vigente en virtud de la ejecución del proyecto.
- Al inicio del proyecto se debe definir el tiempo que la información será utilizada, los periodos de conservación y la accesibilidad.
- Incluir los aspectos de seguridad, privacidad de la información y seguridad digital, y los datos personales en el análisis de riesgos previo al proyecto. Teniendo en cuenta los datos personales recolectados.
- Si el proyecto involucra la contratación de terceros se debe suscribir un documento compromiso de confidencialidad, el cual deberá ser entregado al responsable del proyecto.
- Si el proyecto incluye el desarrollo de sistemas de información, se deben establecer buenas prácticas de desarrollo seguro al inicio del proyecto.

- Los terceros que participan en los proyectos deben divulgar periódicamente al interior de los equipos de trabajo las políticas de seguridad y privacidad de la información y seguridad digital, y de tratamiento de datos personales adoptadas por la Unidad.
- Si el proyecto involucra terceros se debe prever un plan de recuperación y contingencia al inicio del proyecto, ante los eventos que puedan afectar el cumplimiento de la ejecución del proyecto de acuerdo con su objeto.
- Se debe contemplar que en el momento que se presente un incidente de seguridad y privacidad de la información y seguridad digital, este sea reportado al responsable del proyecto.
- El asesor de Planeación, y el Oficial de seguridad y privacidad de la información, deberán apoyar cuando se requiera en la evaluación de los riesgos de seguridad y privacidad de la información en una fase inicial del proyecto para identificar los controles necesarios, de acuerdo con el tipo de proyecto.
- El Oficial de seguridad y privacidad de la información de manera autónoma revisará el cumplimiento e implementación de los requerimientos y consideraciones en materia de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la metodología de gestión de proyectos de la entidad.

Control SI-A.5.9 Inventario de información y otros activos asociados

- El Oficial de seguridad y privacidad de la información en conjunto con la Subdirección de Gestión Corporativa (Gestión Documental), deben diseñar o actualizar una metodología para la identificación, clasificación, valoración y buen uso de los activos de información.
- Todas las dependencias de la Unidad deben contar con un inventario de sus activos de información y se debe evidenciar a través de los instrumentos dispuestos.
- El Oficial de seguridad y privacidad de la información debe consolidar los inventarios reportados por los procesos en un instrumento único que contenga todos los activos de información de la Entidad.
- El Oficial de seguridad y privacidad de la información debe extraer del inventario de activos de información de la Unidad lo requerido para el reporte del índice de transparencia, de acuerdo con lo establecido en los instrumentos de gestión de la información adoptados mediante la Resolución No. 10028 de 2020; para la publicación es necesario que cuente con la validación del asesor de Jurídica en el marco de la clasificación de la información (Pública, Clasificada y Reservada).
- La Subdirección de Información debe identificar los ciberactivos (activos de seguridad digital) críticos con base en los activos definidos en el análisis de impacto en el negocio (BIA). Estos ciberactivos son aquellos que contienen, trasmiten o procesan información de los servicios esenciales de la Entidad.
- Las firmas de documentos oficiales y que se constituye como activos de información de acuerdo con la tabla de retención documental o acto administrativo deben reposar en original o con firma digital del

sistema de gestión documental, en ningún caso se debe utilizar firmas facsímil, digitalizadas o escaneadas, salvo en aquellos que se autorice por resolución expedida por la Dirección, indicando para que fin y porqué medios podrá ser utilizada.

Control SI-A.5.10 Uso aceptable de la información y otros activos asociados

- La Subdirección de Información debe cumplir con los requerimientos de uso, manipulación y conservación de los medios tecnológicos para el almacenamiento de información dadas por el fabricante, con el fin de mantener la disponibilidad e integridad de la información.
- La Subdirección de Gestión Corporativa debe crear o actualizar si fuere necesario el procedimiento o documento donde se establezca la disposición final de residuos de aparatos eléctricos y electrónicos (RAEE).

Control SI-A.5.11 Devolución de activos

Los empleados públicos y contratistas de la Unidad una vez finalizada su vinculación o terminación contractual deben hacer entrega de los activos bajo su responsabilidad de acuerdo con los procedimientos establecidos por la Subdirección de Gestión Corporativa.

Control SI-A.5.12 Clasificación de la información

- La metodología de clasificación de información de la Unidad hará parte integral de la metodología para la identificación, clasificación, valoración y buen uso de los activos de información, que trata el lineamiento en el código SI-A.5.9.
- Los colaboradores deben aplicar la clasificación de la información adoptada por la Entidad, de acuerdo con el inventario de activos de información, el índice de información clasificada y reservada, y la documentación pertinente para el rotulado de la información.
- Cada propietario de los activos de información debe velar por el cumplimiento de la clasificación de acuerdo con lo establecido en la documentación pertinente.

Control SI-A.5.13 Etiquetado de la información

El Oficial de Seguridad y Privacidad de la información en conjunto con el Subdirección de Gestión Corporativa (Gestión Documental), deben diseñar la documentación pertinente para el etiquetado o rotulado de la información física y digital de acuerdo con lo establecido en la normativa sobre información pública y protección de datos personales.

Control SI-A.5.14 Transferencia de información

- Para el intercambio de información se debe tener en cuenta la clasificación para su debida protección en términos de confidencialidad, integridad y privacidad.
- Los colaboradores y terceras partes que interactúen en procesos de intercambio de información deben cumplir los lineamientos, recomendaciones o estrategias establecidas por la Subdirección de Información con el fin de garantizar su recuperación en caso de desastre.
- La Subdirección de Información debe contar con los lineamientos para proteger la información transferida con respecto a la interceptación, copiado, modificación, enrutado y destrucción de esta.
- La Subdirección de Información debe establecer procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas.
- La Subdirección de Información debe establecer controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico de la Unidad.
- La Subdirección de Gestión Corporativa debe dictar directrices sobre retención, disposición y transferencia de la información física y/o electrónica de la Unidad, de acuerdo con la legislación y reglamentaciones local y nacional aplicable.
- Para la transferencia de información entre la Unidad y las partes externas se debe establecer un acuerdo donde se definan las condiciones legales, técnicas y procedimentales.
- La Subdirección de Información debe establecer mecanismos para el direccionamiento y transporte correcto del mensaje, así como la confiabilidad y disponibilidad del servicio.
- La Subdirección de Información debe proporcionar herramientas de mensajería electrónica corporativas, como mensajería instantánea y redes sociales en conjunto con el área de comunicaciones.
- Cuando se requiera transferir un medio de almacenamiento de información de la Unidad a otras entidades se deben establecer un acuerdo entre las partes. Dichos acuerdos deben dirigirse a la transferencia segura de información de interés entre la Unidad y las partes.
- El transporte para los medios de almacenamiento debe contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información de la Unidad.
- La Unidad debe implementar en las áreas seguras donde se maneje información reservada o nivel de confidencialidad alto, controles adecuados que las permitan aislar acústicamente.

Control SI-A.5.15 Control de acceso

- La Subdirección de Información debe suministrar a los usuarios las credenciales para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados; las credenciales de acceso son de uso personal e intransferible.

- La conexión remota a servicios específicos de infraestructura tecnológica a los cuales se acceden a través de la red de área local de la Unidad debe establecerse a través de una conexión VPN, la cual deberá ser aprobada, registrada y monitoreada por la Subdirección de Información; además, se debe mantener una relación de las VPN con su respectivo ticket de creación.
- La Subdirección de Información debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servicios.
- La Subdirección de Información debe establecer para el control de acceso a los datos, información y servicios el principio del menor privilegio y la necesidad de conocer, lo que implica que no se otorgará acceso a menos que sea explícitamente autorizado.
- La Subdirección de Información debe verificar periódicamente los controles de acceso para los usuarios de la Unidad y los provistos a terceras partes, con el fin de revisar que dichos usuarios tengan los permisos únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.
- La Subdirección de Información debe revisar que los equipos personales de los colaboradores que se conecten a las redes de datos de la Unidad cumplan con todos los requisitos o controles para autenticarse y únicamente podrán realizar las tareas para las que fueron autorizados.
- La Subdirección de Información debe controlar el uso de conexiones a través de proxys anónimos o técnicas similares, a fin de minimizar los riesgos de seguridad digital de estas técnicas.

Control SI-A.5.16 Gestión de identidad

- La Subdirección de Información debe definir mecanismos para la inhabilitación de usuarios para el acceso a los recursos de tecnologías de la información de la Unidad, teniendo en cuenta que las identificaciones de los usuarios deberán ser únicas.
- La Subdirección de Información debe definir un estándar para la identificación de usuarios, teniendo en cuenta los siguientes parámetros:
  - Usar la primera letra del primer nombre más el apellido, en caso de homónimos se utiliza, la primera letra del primer nombre más la primera letra del segundo nombre más el apellido, de persistir la situación, se deberá utilizar la primera letra del primer nombre más el apellido, seguido de la primera letra del segundo apellido; si todas las opciones anteriores se encuentra en uso, se utilizará la primera letra del primer nombre más la primera letra del segundo nombre más el primer apellido más la primera letra del segundo apellido.
  - El nombre para mostrar debe ser los nombres y apellidos completos. El usuario de correo electrónico debe ser igual al usuario de red, es decir, debe existir interoperabilidad entre el servicio de correo y el directorio activo (DA).

- La Subdirección de Información solo otorgará a los usuarios accesos solicitados y autorizados por el jefe inmediato o supervisor del contrato.
- Solo se debe otorgar los privilegios para la administración de recursos tecnológicos, servicios de red, sistema operativo y sistemas de información únicamente a aquellos colaboradores que cumplan dichas funciones, deben ser cuentas únicas asociadas al usuario de dominio del colaborador; en caso de requerirse usuarios de acceso genérico, éstos deben ser entregados al colaborador de manera formal por parte del jefe inmediato o supervisor del contrato; en caso de cambiar el titular de la cuenta genérica la contraseña de acceso debe ser modificadas de manera inmediata.

- Los usuarios administradores de recursos tecnológicos, servicios de red, sistema operativo y sistemas de información, entre otros, tienen la responsabilidad de entregar para la custodia todas las cuentas y claves administradoras bajo su responsabilidad.
- Se debe restringir las conexiones remotas para la administración de la plataforma tecnológica; únicamente se deberá permitir el acceso a los colaboradores autorizados por la Subdirección de Información.

Control SI-A.5.17 Información de autenticación

- La Subdirección de Información debe deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos.
- La Subdirección de Información debe mantener un listado actualizado con las cuentas que administren todos los recursos tecnológicos.
- La contraseña para la autenticación o los números de identificación personal (PIN) generados automáticamente se debe suministrar a los usuarios de manera segura, y el sistema debe forzar a los usuarios a cambiar sus contraseñas en el primer inicio de sesión.
- Se debe establecer mecanismos para verificar la identidad de un usuario antes de reemplazar la información secreta para la autenticación o proporcionar una nueva o temporal.
- La Subdirección de Información debe generar reportes de uso de cada uno de los sistemas de información o recursos tecnológicos con el fin de identificar la periodicidad de uso de los usuarios, en caso de identificar inactividad mayor o igual a 15 días hábiles se bloqueará el usuario y se debe realizar validación con el área a la que pertenece para determinar si se procede a la desactivación definitiva o temporal por novedad.
- El cambio de contraseña solo podrá ser solicitada por el titular de la cuenta, su jefe inmediato o supervisor del contrato.
- Los usuarios deben usar contraseñas seguras, es decir:
  - Poseer algún grado de complejidad y no deberán ser palabras comunes que se puedan encontrar

en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, cónyuge o, mascotas, placas de automóvil, fechas de aniversarios, cumpleaños, nombre de usuario, el nombre real o las siglas UNIDAD, UAPA, etc.
    - No usar las mismas contraseñas de autenticación laboral para uso personal.
    - Debe cambiarse, por ejemplo, después de un incidente de seguridad o al terminar o cambiar de empleo cuando un usuario tiene contraseñas conocidas para usuarios que permanecen activos.
    - No registrar en papel, correo electrónico, archivos digitales a menos que se puedan almacenar de forma segura y el método de almacenamiento esté aprobado por la Subdirección de Información.
- La contraseña debe cumplir con las siguientes recomendaciones como mínimo:
    - Tener como mínimo nueve (8) caracteres con las siguientes características:
    - Alfanumérica sin repetición.
    - Deben ser diferentes de otras contraseñas anteriores proporcionadas, es decir las ultimas diez (10) suministradas al dominio no se deberán repetir.
    - Deben estar compuestas por: letras en mayúsculas “A, B, C…”, letras en minúsculas “a, b, c…”, números “0, 1, 2, 3…”, símbolos especiales “@, #, $, %, &, (), ¡, !¡, ¿,?, <>…” en cualquier combinación.
    - Debe cambiarse obligatoriamente cada 45 días.
    - Después de 3 (tres) intentos no exitosos de ingreso de la contraseña el usuario deberá ser bloqueado de manera inmediata y deberá esperar un tiempo determinado de 3 minutos para volver a intentar, o solicitar el desbloqueo a través de la Mesa de servicios.
    - No debe ser visible en la pantalla, al momento de ser ingresada.

Control SI-A.5.18 Derechos de acceso

- La Subdirección de Información debe revisar los derechos de acceso de los usuarios administradores por lo menos dos veces al año.
- Para realizar el ajuste o retiro de los derechos de acceso se debe tener en cuenta lo establecido en el control SI-A.6.5 de este documento.
- La Subdirección de Información debe establecer mecanismos para la creación, asignación y custodia de contraseñas de los usuarios superadministradores de las herramientas de administración que se crean para configurar los servicios de la operación tecnológica de la Unidad, teniendo en cuenta las siguientes recomendaciones para establecerla de manera segura:
    - Poseer un nivel de complejidad alto y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, cónyuge o mascotas, placas de automóvil, fechas de aniversarios, cumpleaños, nombre de

usuario, el nombre real o las siglas UNIDAD, UAPA, etc.

- Tener como mínimo veinte (20) caracteres con las siguientes características:
- Alfanumérica sin repetición.
- Estar compuestas por: letras en mayúsculas “A, B, C…”, letras en minúsculas “a, b, c…”, números “0, 1, 2, 3…”, símbolos especiales “@, #, $, %, &, (), ¡, !, ¿, ?, <>…” en cualquier combinación.
- No registrar en papel, correo electrónico, archivos digitales a menos que se puedan almacenar de forma segura.
- Cambiarse si se ha detectado anomalías en la cuenta de usuario o si alguna de las partes (subdirector, administrador o líder del servicio) cambia de área o se desvincula de la Unidad.

Control SI-A.5.19 Seguridad de la Información en las relaciones con los proveedores

- La Subdirección de Gestión Corporativa (Gestión Contractual) debe establecer en el momento de suscribirse contratos de cualquier tipo los riesgos asociados a la seguridad y privacidad de la información y seguridad digital, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad y privacidad de la información de la Unidad.
- La Subdirección de Información debe establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica de la Unidad.

Control SI-A.5.20 Seguridad de la Información en los acuerdos con los proveedores

- La Subdirección de Gestión Corporativa (Gestión Contractual) debe establecer lineamientos para el cumplimiento de las obligaciones contractuales del Sistema de Gestión de Seguridad y Privacidad de la Información con terceros o proveedores.
- La Subdirección de Gestión Corporativa (Gestión Contractual) deberá establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
- La Subdirección de Información debe verificar mensualmente el cumplimiento de Acuerdos de Nivel de Servicio establecidos con sus proveedores de tecnología.

Control SI-A.5.21 Gestión de la SI en la cadena de suministro TIC

- Cada dependencia de la Unidad que establezca relación con proveedores y su cadena de suministro TIC, debe solicitar acompañamiento a la Subdirección de Información con el fin de dar a conocer los

requisitos de seguridad de la información y seguridad digital que tiene la Unidad y que son aplicables a la adquisición de productos o servicios TIC.

Control SI-A.5.22 Monitoreo, revisión y gestión de cambios de los servicios de proveedores

- La Subdirección de Gestión Corporativa (Gestión Contractual) debe documentar las obligaciones generales sobre seguridad y privacidad de la información, seguridad digital y continuidad de la operación, para la verificación de estas por parte del supervisor de contrato.
- La Subdirección de Información debe establecer un mecanismo que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en la gestión de cambios.

Control SI-A.5.23 Seguridad de la Información para el uso de servicios en la nube

- La Subdirección de Información debe definir los requisitos de seguridad y privacidad de la información, y gestionar los riesgos asociados con el uso de servicios en la nube.
- La Subdirección de Información debe verificar mensualmente el cumplimiento de acuerdos de servicio establecidos con sus proveedores de servicios en la nube.

Control SI-A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

La Subdirección de Información en conjunto con el Oficial de seguridad y privacidad de la información deben definir, establecer y comunicar procesos, los roles y responsabilidades para la gestión de incidentes de seguridad y privacidad de la información y seguridad digital.

Control SI-A.5.25 Evaluación y decisión sobre eventos de seguridad de la información

La Subdirección de Información en conjunto con el Oficial de seguridad y privacidad de la información es la encargada en primera instancia de evaluar y atender los eventos de seguridad y privacidad de la información y de tomar decisiones sobre los mismos, así como de categorizarlos como incidentes de acuerdo con los criterios establecidos. En caso de requerir apoyo o asesoría externa de autoridades o profesionales especializados en seguridad se debe solicitar a través del subdirector de información en conjunto con el Oficial de seguridad y privacidad de la información.

Control SI-A.5.26 Respuesta a incidentes de seguridad de la información

- La Subdirección de Información en conjunto con el Oficial de seguridad y privacidad de la información deben responder a los incidentes de seguridad de la información de conformidad con el procedimiento MST-PR-02 publicado en la Intranet.
- La Subdirección de Información en conjunto con el Oficial de seguridad y privacidad de la información deben contar con los mecanismos para el cumplimiento de los tiempos en la respuesta a los incidentes de seguridad y privacidad de la información y seguridad digital.

Control SI-A.5.27 Aprendizaje de los incidentes de seguridad de la información

La Subdirección de Información en conjunto con el Oficial de seguridad y privacidad de la información deben proporcionar los medios para la gestión de conocimiento de los incidentes de seguridad y privacidad de la información y seguridad digital presentados, reduciendo de esta manera la probabilidad o las consecuencias de futuros incidentes.

Control SI-A.5.28 Recopilación de evidencia

- La Subdirección de Información en conjunto con el Oficial de seguridad y privacidad de la información serán los encargados de la recolección de evidencias de los incidentes de seguridad y privacidad de la información y seguridad digital. Deberá seguir los lineamientos para la recolección de evidencias de elementos informáticos como primer respondiente.
- La Subdirección de Información en conjunto con el Oficial de seguridad y privacidad de la información deben definir los mecanismos para la recolección de evidencias de elementos informáticos, con el fin de garantizar la autenticidad de los elementos materiales de prueba recolectados y examinados, asegurando que pertenecen al caso investigado, sin confusión, adulteración o sustracción.

Control SI-A.5.29 Seguridad de la información durante una interrupción

- Se debe estructurar el Plan de continuidad de la operación acorde al alcance del sistema de gestión de seguridad y privacidad de la Información en coordinación con los líderes de los procesos y conforme a la normativa interna vigente.
- El asesor de Planeación en conjunto con el oficial de seguridad y privacidad de la información y la Subdirección de Información deben diseñar una metodología para la identificación y evaluación de riesgos de continuidad de la operación de los servicios de la Unidad.

- El plan de continuidad del negocio debe ser revisado en sesión del Comité institucional de gestión y desempeño, como mínimo una vez al año o cuando ocurra un cambio en el contexto interno o externo de la Unidad.
- La Subdirección de Información debe disponer de planes de contingencia de los servicios de TIC y un plan de recuperación ante desastres, enfocados a lograr el retorno a la operación normal.
- La Subdirección de Gestión Corporativa (Gestión Contractual) debe incluir en los procesos contractuales una obligación general que exija a los contratistas a disponer de planes de contingencia y se deberá analizar su cobertura y alcance.
- El Plan de Continuidad de la Operación debe ser comunicado al interior de la Unidad.
- En caso de presentarse un incidente significativo que conlleve a una interrupción se deberá gestionar el manejo de la crisis y los mecanismos de comunicación apropiados tanto internos como externos durante el estado de contingencia.
- La Subdirección de Gestión Corporativa debe garantizar la integración de los planes de emergencia y contingencia con el plan de continuidad de la operación de los servicios de la Unidad.
- Se deben ejecutar procedimientos de control de cambios según las acciones preventivas y correctivas que se generaron a partir de las pruebas, para asegurar que el Plan de Continuidad se mantenga actualizado y mejorado.

Control SI-A.5.30 preparación de las TIC para la continuidad del negocio

- La Alta Dirección en conjunto con el Oficial de seguridad y privacidad de la Información y Subdirección de Información deben desarrollar un análisis de impacto al negocio (BIA por sus siglas en inglés), por medio del cual se identifiquen los servicios críticos de la Unidad.
- La Alta Dirección en conjunto con el oficial de seguridad y privacidad de la Información y la Subdirección de Información deben realizar un plan de pruebas del plan de continuidad de la operación y deberá ser ejecutado mínimo 2 veces al año.
- La Subdirección de Información debe definir un equipo para la planeación de pruebas, los procesos que estarán involucrados, la infraestructura tecnológica y/u operativa requerida, el plan de rollback y las actividades a realizar. Los participantes de los equipos deberán recibir sensibilización con respecto a los procesos, sus roles y responsabilidades en caso de incidente o desastre.
- El equipo de pruebas del plan de continuidad debe documentar las pruebas y generar reportes o informes después de cada prueba y/o ejercicio que incluya recomendaciones, lecciones aprendidas y acciones para mejorar el plan y presentarlas al Comité institucional de gestión y desempeño.
- La Alta Dirección en conjunto con el Oficial de seguridad y privacidad de la Información y la Subdirección de Información, en coordinación con los líderes de procesos deben diseñar y aprobar las estrategias y

tiempos de recuperación de la operación de los servicios críticos de la Unidad.

Control SI-A.5.31 Requisitos legales, reglamentarios y contractuales

- El Oficial de seguridad y privacidad de la información en conjunto con el asesor Jurídico deben identificar, documentar y actualizar todos los requerimientos contractuales, estatutarios y reglamentarios utilizando una herramienta para la verificación de dichos requisitos.
- El Oficial de seguridad y privacidad de la información de la información en coordinación con las dependencias responsables, debe definir y establecer un procedimiento que contemple la revisión y verificación del cumplimiento de los requisitos legales, reglamentarios y contractuales en materia de seguridad y privacidad de la información.

Control SI-A.5.32 Derechos de propiedad intelectual

- La Unidad debe aplicar procedimientos apropiados para el cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con los derechos de autor y propiedad intelectual, en los procesos de selección.
- La Subdirección de Información en conjunto el aseso Jurídico deben definir controles con el objetivo de proteger adecuadamente la propiedad intelectual, tales como derechos de autor de software, licencias, manuales y código fuente. El material registrado con derechos de autor no se debe copiar sin la autorización del propietario.
- La Subdirección de Información debe asegurar y controlar la cantidad permitida de licencias o recursos para los usuarios, adicionalmente, debe llevar a cabo revisiones periódicas para asegurar que solo se instale software autorizado y productos con licencia.
- El Oficial de seguridad y privacidad de la Información en conjunto con el asesor de comunicaciones debe generar campañas de comunicación con el fin de apropiar a los colaboradores de la Unidad sobre el uso de los derechos de propiedad intelectual (no copiar total ni parcialmente libros, artículo u otros documentos diferentes de los permitidos por la ley de derechos de autor).

Control SI-A.5.33 Protección de los registros

- La Subdirección de Gestión Corporativa (Gestión Documental) debe generar directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información física y digital de la Unidad.
- La Subdirección de Gestión Corporativa (Gestión Documental) en conjunto con la Subdirección de Información deben establecer e implementar controles para proteger los registros contra pérdida,

accesos no autorizados, destrucción y falsificación de información física y digital.

- La Subdirección de Gestión Corporativa (Gestión Documental) en conjunto con la Subdirección de Información deben establecer procedimientos de almacenamiento a largo plazo y manipulación de los registros físicos y digitales.
- La Subdirección de Gestión Corporativa (Gestión Documental) deberá disponer de un sistema de gestión documental electrónica y de archivo digital, asegurando la conformación de expedientes electrónicos con características de integridad, disponibilidad, usabilidad y autenticidad de la información.

Control SI-A.5.34 Privacidad y protección de la IIP

- El Oficial de seguridad y privacidad de la información y el asesor Jurídico, deben definir o actualizar cuando sea necesario la política de tratamiento de datos personales, para la protección de los derechos fundamentales de la información de las partes interesadas pertinentes en relación con su tratamiento.
- La Unidad a través del Oficial de seguridad y privacidad de la información, deberá disponer los lineamientos para la protección de la información de los empleados públicos, contratistas y grupos de interés externos, en los términos de la Ley 1581 de 2012 y de acuerdo con lo estipulado en la Política de tratamiento de datos personales de la entidad.
- La Unidad deberá designar un funcionario o área y les asignará las funciones que ejercerá como oficial de protección de datos personales, quien proporcionará guía al personal, proveedores de servicios y otras partes interesadas sobre sus responsabilidades individuales y los procedimientos específicos a seguir frente al tratamiento y protección de los datos personales.

Control SI-A.5.35 Revisión independiente de la Seguridad de la Información

- La Subdirección de Gestión Corporativa (Gestión Contractual) debe incluir los mecanismos para que los supervisores de contrato validen el cumplimiento de las obligaciones generales en materia de seguridad y privacidad de la información.
- El líder del Sistema de gestión de Seguridad y privacidad de la información en el caso que se necesite incluir y/o reprogramar un ciclo de auditoría interna al Sistema de Seguridad de la Información en el Programa Anual de Auditoría (PAA), al inicio de cada vigencia, deberá hacer la solicitud al asesor de Control Interno, para que se coordine su programación y sea aprobado en el Comité Institucional de Coordinación de Control Interno. Lo anterior teniendo en cuenta lo establecido en la Guía de auditoría interna basada en riesgos para entidades públicas del DAFP.

Control SI-A.5.36 Cumplimiento de políticas, normas y estándares de Seguridad de la Información

- Los líderes de los procesos deberán asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas. Los resultados de estas revisiones serán mantenidos para su revisión en auditorías.
- La Subdirección de Información debe comprobar periódicamente que los sistemas de información cumplen con las normas de implementación de seguridad. Se deberán realizar auditorías periódicas y generar informes técnicos.

Control SI-A.5.37 Procedimientos operativos documentados

- La Subdirección de Información con el apoyo del asesor de Planeación debe documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad, confidencialidad y privacidad de la información.
- La Subdirección de Información debe poner a disposición de todos los colaboradores los procedimientos de operación mediante los medios que la Unidad disponga.

6.1.2 Controles para el Recurso Humano

Control SI-A.6.1 Selección

- La Subdirección de Gestión Corporativa (Gestión de Talento Humano) debe definir formalmente un mecanismo de verificación del personal en el momento en que se postula al cargo. Dicho mecanismo deberá incluir los aspectos legales y procedimentales de vinculación a la Unidad y los que dicte la Función Pública. Para vinculaciones que deban manejar información confidencial, también debería considerarse la posibilidad de realizar verificaciones adicionales más detalladas.
- La Subdirección de Gestión Corporativa (Gestión Contractual) debe definir una lista de verificación que contengan los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con lo que dicta la ley y la reglamentación vigente. Para contrataciones que deban manejar información confidencial, también debería considerarse la posibilidad de realizar verificaciones adicionales más detalladas.
- Los procesos de selección de personal de empleados públicos y contratistas de prestación de servicios deben contener la autorización para el tratamiento de los datos personales acorde con la Política de tratamiento de datos personales de la Unidad, y de acuerdo con lo establecido en la Ley 1581 de 2012

y sus decretos reglamentarios.

- La Subdirección de Gestión corporativa (Gestión de Talento Humano y Gestión Contractual) en conjunto con la Gestión Documental deben establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en los expedientes contractuales e historias laborales.

Control SI-A.6.2 Condiciones del empleo

- La Subdirección de Gestión Corporativa (Gestión de Talento Humano) debe incluir dentro del manual de funciones las responsabilidades con respecto al cumplimiento de las políticas de seguridad y privacidad de la información y seguridad digital, así como todos los lineamientos en el marco del Sistema de gestión de seguridad y privacidad de la Información.
- La Subdirección de Gestión Corporativa (Gestión Contractual) debe incluir en los estudios previos, así como en la minuta contractual, las obligaciones referentes a las políticas, lineamientos y directrices en materia de seguridad y privacidad de la información y seguridad digital que dicte la Unidad.
- La Subdirección de Gestión Corporativa (Gestión de Talento Humano y gestión Contractual) deben dar a conocer durante la inducción las responsabilidades u obligaciones en materia de la seguridad y privacidad de la información y seguridad digital y aclarar que estas se extienden más allá de los límites de la Unidad, del horario normal de trabajo o de la ejecución del objeto contractual; incluidas aquellas responsabilidades a tener frente al manejo de la información recibida de las partes interesadas.
- Una vez formalizado el proceso de vinculación o contratación, el jefe inmediato, supervisor o el delegado de la dependencia para tal fin, debe solicitar la activación del usuario, la apertura del inventario y demás servicios que requiera el colaborador para la ejecución de sus funciones u obligaciones contractuales.

Control SI-A.6.3 sensibilización, educación y formación en SI

- El Oficial de seguridad y privacidad de la información en conjunto con el asesor de comunicaciones deben diseñar e implementar un programa para el cambio y cultura organizacional en apropiación del SGSPI, el cual se debe ejecutar durante la vigencia al interior de la Unidad.
- La Subdirección de Gestión Corporativa (Gestión de Talento Humano) o el supervisor del contrato deben propender porque los colaboradores de la Unidad y usuarios de terceras partes que desempeñen funciones reciban entrenamiento y actualización periódica en materia de seguridad y privacidad de la información y seguridad digital.
- La Subdirección de Gestión Corporativa (Gestión de Talento Humano) en conjunto con el Oficial de seguridad y privacidad de la información, deben contemplar capacitaciones (internas o externas)

relacionadas con seguridad y privacidad de la información y seguridad digital.

Control SI-A.6.4 Proceso disciplinario

En lo pertinente al incumplimiento y desacato de las políticas de la seguridad y privacidad de la información y seguridad digital, se aplicará lo establecido por los entes de control interno disciplinario de la Unidad, enmarcados en la Ley 1952 de 2019 para empleados públicos y Ley 1474 de 2011 para contratistas, sus decretos reglamentarios o cualquiera que la modifique, adicione, derogue o subrogue.

Control SI-A.6.5 Responsabilidades después del término o cambio de empleo

- El jefe inmediato o a quien este delegue debe recoger y custodiar la información propia de la Unidad que se encuentra en gestión del empleado público, cuando existe una novedad de retiro, investigación, inhabilidades, o cambio de funciones.
- El supervisor del contrato o a quien este delegue debe recoger y custodiar la información de la Unidad bajo la responsabilidad del contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
- La Subdirección de Información debe parametrizar en el directorio activo, la inactivación automática de los contratistas, teniendo en cuenta la fecha de terminación del contrato; la inactivación de los usuarios de los sistemas de información que no se autentican con el directorio activo, se debe hacer de forma manual.
- La Subdirección de Gestión Corporativa (Gestión de Talento Humano y Gestión Contractual) deberán informar a la Subdirección de Información a través de la mesa de servicios, cualquier novedad de desvinculación administrativa, laboral o contractual del colaborador; una vez notificada la novedad, la Subdirección de Información deberá proceder a la inactivación de los accesos del colaborador, teniendo en cuenta los siguientes parámetros:
  - Si el buzón pertenece a una cuenta de correo genérica (ejemplo: info@uapa-pae.gov.co), a este se le deberá cambiar la contraseña inmediatamente y asignar nuevo responsable para evitar accesos no autorizados.
  - En caso de que el buzón sea objeto de investigación por parte de las autoridades competentes, se les entregará en cadena de custodia una copia del buzón garantizando su integridad. Se deben inactivar los accesos biométricos o de tarjetas de proximidad de los sistemas de control de acceso.
  - Para el buzón de correo electrónico se creará una copia de respaldo una vez se dé por terminada la vinculación con la Unidad.
- Bajo ningún parámetro se podrán restablecer los accesos a estas cuentas; solo se podrán restablecer buzones en ambientes offline y aquellos que por solicitud directa del jefe inmediato o supervisor de

contrato lo justifique, y no se podrán emitir correos ni notificaciones desde estos buzones.

- Se deben inactivar todos los accesos a los sistemas de información.
- Se debe solicitar la devolución del carné o cualquier distintivo de autenticación o prenda de vestir, que lo acredita como colaborador de la Unidad.
- Cuando un empleado público o contratista cesa en sus funciones o culmina la ejecución de contrato con la Unidad, no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa de la dirección de la Unidad, por orden judicial o por solicitud de Control interno disciplinario como parte de un proceso de investigación.
- Cuando un empleado público de la Subdirección de Información cambia de funciones, área o dependencia y su vínculo laboral sigue vigente, se podrá generar una copia de su buzón institucional. La Subdirección de Información deberá crear un nuevo usuario de directorio activo para que el empleado público pueda asumir su nuevo rol.

Control SI-A.6.6 Acuerdos de confidencialidad o no divulgación

- Todo empleado público o contratista debe firmar un documento o compromiso de confidencialidad y no divulgación de la información con la Unidad, dicho documento debe reposar en la historia laboral o expediente contractual según sea el caso.
- Para el personal externo que ejecute tareas propias de la Unidad y haya sido contratado en el marco de un contrato o convenio con la Entidad, debe firmar un compromiso de confidencialidad y no divulgación de la información con el representante Legal, y este debe reposar en la carpeta de ejecución del contrato.

Control SI-A.6.7 Trabajo remoto

- La Subdirección de Información debe establecer la documentación necesaria que brinde a las dependencias la orientación con respecto a la autorización, configuración y uso de los dispositivos móviles de propiedad de empleados públicos, contratistas o terceros que requieran tener acceso a la información a través de los servicios tecnológicos de la Unidad.
- La Subdirección de Información debe implementar las medidas necesarias de seguridad y privacidad, para propender por la protección de la información gestionada mediante aplicaciones y sistemas de información.
- La Subdirección de Información debe mantener un inventario actualizado de los dispositivos móviles personales autorizados en el marco de la política TTPD para acceder a la red corporativa, asociando el número de ticket de la mesa de servicios por el cual fue autorizada la solicitud.
- La Subdirección de Información debe establecer los mecanismos técnicos u operativos en aras de

garantizar que los computadores portátiles personales, cuenten con software licenciados y antivirus actualizado.

- Los computadores portátiles de propiedad de los colaboradores no deberán estar incluidos en el dominio uapa-pae.gov.co o cualquiera que funcione dentro de la Unidad. Para conectarse a los servicios de la red de datos deberán realizar solicitud a la mesa de servicios y cumplir con los lineamientos referentes a seguridad y privacidad de la información y seguridad digital.
- La Subdirección de Información debe proporcionar a los dispositivos móviles, las herramientas ofimáticas y de almacenamiento en nube licenciadas por la Entidad.
- Para la modalidad de teletrabajo, la Subdirección de Información debe definir y proveer las herramientas tecnológicas para teletrabajar, estableciendo las condiciones de seguridad y privacidad de la información y seguridad digital, de acuerdo con la normativa vigente en la materia o cualquiera que la adicione, modifique o complemente.
- La Subdirección de Gestión Corporativa (Gestión de Talento Humano) debe mantener actualizado la documentación de teletrabajo y trabajo en casa y en especial los aspectos relacionados con la seguridad y privacidad de la información y seguridad digital.
- La Subdirección de Gestión Corporativa (Gestión de Talento Humano) debe establecer los mecanismos necesarios para sensibilizar a los teletrabajadores y aspirantes a teletrabajo en temas de seguridad y privacidad de la información y seguridad digital.
- Para la modalidad de Teletrabajo, la Subdirección de Información debe establecer mecanismos de monitoreo sobre las conexiones y los servicios tecnológicos a los que el teletrabajador tiene acceso.

Control SI-A.6.8 Informes de eventos de SI

- La Subdirección de Información debe definir los canales para que los colaboradores de la Unidad puedan reportar los incidentes de seguridad y privacidad de la información y seguridad digital.
- La Subdirección de Información en conjunto con el Oficial de seguridad y privacidad de la información, La Subdirección de Gestión Corporativa (Gestión de Talento Humano) y el área de comunicaciones deben dar a conocer a los colaboradores de la Unidad los lineamientos establecidos para la gestión de incidentes de seguridad y privacidad de la Información.

6.1.3 Controles para la Protección Física

Control SI-A.7.1 Perímetros de seguridad física

- La Subdirección de Gestión Corporativa debe definir y establecer un sistema de control de acceso a las instalaciones de la Unidad, así como a las áreas seguras identificadas, con el fin de evitar el acceso físico no autorizado, los daños y las interferencias en la información de la organización y otros activos asociados.
- El asesor de control interno de acuerdo al PAAI (Programa Anual de Auditoría Interna, aprobado por el Comité Institucional de Coordinación de Control Interno) y una vez establecido que la revisión del estado del centro de cableado es de alto riesgo, debe contemplar como un objetivo la revisión del estado de estos espacios e informar cualquier anomalía presentada de la siguiente manera: daños en el rack y equipos activos de red a la Subdirección de Información, y daños en infraestructura física (puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, biométricos, entre otros) a la Subdirección de Gestión Corporativa.

Control SI-A.7.2 Entrada física

- Todos los puntos de acceso deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o instalación.
- El personal de vigilancia debe registrar en una bitácora o sistema de información el ingreso y retiro de todo equipo de cómputo (PC o portátil, mouse, teclado, cargador, etc.), servidores, equipos activos de red o cualquier equipo electrónico diferentes a celular; en caso de que estos equipos sean de propiedad de la Unidad, deberán contar con autorización expresa de la Subdirección de Gestión Corporativa o Subdirección de Información según sea el caso y de acuerdo con los procedimientos establecidos para tal fin.
- El personal de vigilancia debe establecer mecanismos para inspeccionar y examinar los morrales, bolsos, cajas, etc., que ingresen los colaboradores o visitantes.

Control SI-A.7.3 Protección de oficinas, salas e instalaciones

- La Subdirección de Información debe controlar el ingreso a los centros de datos o centros de cableado de la Unidad.
- La Subdirección de Información será la encargada de autorizar el ingreso a personal ajeno a la Unidad a los centros de datos o centros de cableado, este deberá estar acompañado por quien sea autorizado,

y se hará responsable de la estadía del personal ajeno a la entidad durante el tiempo que permanezca en las instalaciones.

- La Subdirección de Gestión Corporativa es responsable de la identificación y organización del cableado estructurado desde los puestos de trabajo hasta los paneles de conexión (patch panel) de los centros de cableado.
- La Subdirección de Gestión Corporativa debe mantener en buen estado la infraestructura física de los centros de cableado o centros de datos de la Unidad, tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, sensores, biométricos, entre otros.

Control SI-A.7.4 Monitoreo de la seguridad física

- El perímetro de seguridad de las áreas seguras debe contar con vigilancia mediante CCTV y debe ser monitoreado permanentemente por el personal de vigilancia.
- El trabajo en áreas seguras debe estar monitoreado por CCTV, teniendo en cuenta que las cámaras no podrán apuntar directamente a la captura de información dentro de estas áreas.
- La Subdirección de Gestión Corporativa debe respaldar los videos generados por las cámaras de vigilancia e información generada de los accesos a las instalaciones de la Unidad de acuerdo con las políticas de respaldo de la información de la entidad.
- La Subdirección de Gestión Corporativa debe considerar las leyes y normativas locales, incluida la protección de datos personales, en los mecanismos adoptados para la supervisión y grabación a la supervisión del personal y los períodos de retención de estas.

Control SI-A.7.5 Protección contra amenazas físicas y ambientales

- La Subdirección de Gestión Corporativa en conjunto con la Subdirección de Información establecerán los lineamientos para los controles contra amenazas físicas y ambientales como los desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura, estos quedarán enmarcados en los planes de contingencia, de emergencia y de continuidad de los servicios prestados por la entidad.
- La Subdirección de Gestión Corporativa, es la responsable del cumplimiento del protocolo de aseo en los centros de cableado o centro de datos, este último contará con el acompañamiento de Subdirección de Información.
- La Subdirección de Información y la Subdirección de Gestión Corporativa deben mantener libre de objetos o elementos que no sean propios en la operación en el centro de datos o centros de cableado de la Unidad.

- La Subdirección de Información y la Subdirección de Gestión Corporativa en la evaluación de riesgos, deberían identificarse las amenazas físicas y ambientales pertinentes y considerarse los controles apropiados en escenarios de fuego, inundaciones, sobretensiones eléctricas, explosivos y armas.

Control SI-A.7.6 Trabajo en zonas seguras

- En las áreas seguras identificadas se debe restringir el uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello por parte del área encargada, esta prohibición debe estar señalizada.
- Se prohíbe el consumo de alimentos y bebidas en las zonas seguras de la Unidad, esta prohibición debe ser señalizada.
- Las puertas y ventanas de las zonas seguras deberán permanecer cerradas y con llave cuando no hay supervisión o están desocupadas.
- La Subdirección de Información es responsable de mantener organizado e identificado el cableado en los racks de los centros cableado o centro de datos.
- Se debe establecer un plan de mantenimiento locativo para los centros de cableado por parte de la Subdirección de gestión Corporativa y un plan de mantenimiento de los recursos tecnológicos por parte de la Subdirección de Información, de tal manera que se corrijan fallas y/o establecer mejoras en los mismos.
- La Subdirección de Gestión Corporativa debe establecer mecanismos de seguridad para el ingreso a las áreas de procesamiento de pagos y debe ser monitoreado mediante circuito cerrado de televisión (CCTV), que cubra el acceso al área y al funcionario que utilice los equipos financieros, en ningún caso deberá grabarse o monitorear directamente la pantalla o el teclado de los equipos financieros.

Control SI-A.7.7 Escritorio limpio y pantalla limpia

- Los colaboradores de la Unidad, durante su ausencia no deberán conservar sobre el escritorio información propia de la Entidad como documentos físicos o medios de almacenamiento que contengan información clasificada o reservada, por lo tanto, se requiere guardar en un lugar seguro para impedir su pérdida, daño, copia o acceso por parte de terceros o personal que no tenga autorización para su uso o conocimiento.
- La Subdirección de Información debe configurar como política general, que todos los equipos de cómputo que se encuentren en los dominios de la Unidad oculten de manera automática los iconos, accesos directos o documentos que se encuentren en el escritorio. Adicionalmente, todos los equipos y sistemas deberán configurarse con una función de tiempo de espera o cierre de sesión automático.

Control SI-A.7.8 Ubicación y protección de los equipos

- La Subdirección de Gestión Corporativa con el apoyo de la Subdirección de Información propenderán que los equipos de cómputo e impresoras estén situados y protegidos en áreas para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.
- La Subdirección de Información debe propender porque los equipos de cómputo portátiles suministrados por la Entidad se protejan mediante mecanismos que no permitan su pérdida.
- La Subdirección de Gestión Corporativa debe establecer los lineamientos para el uso de la red de energía regulada en los puestos de trabajo en los cuales solo se deben conectar equipos como computadores de escritorio, portátiles y pantallas.
- La Subdirección de Gestión Corporativa debe implementar mecanismos para regular el flujo de energía e interrupciones causadas por fallas en el soporte de los servicios públicos que puedan afectar los equipos de cómputo y procesamiento de información.
- Los puestos de trabajo de los colaboradores de la Unidad y terceras partes que prestan sus servicios y cuyas funciones no obliguen a la atención directa de ciudadanos deberán localizarse preferiblemente en ubicaciones físicas que no estén expuestas al público para minimizar los riesgos asociados al acceso no autorizado de la información o a los equipos informáticos.

Control SI-A.7.9 Seguridad de los activos fuera de las instalaciones

- La Subdirección de Información debe autorizar el uso de los dispositivos de propiedad privada o personales y utilizados para el cumplimiento de las obligaciones o funciones adquiridas en la Unidad.
- En los casos en que los equipos requieran salir de las instalaciones de la Unidad por alguno de los siguientes eventos: reparación, mantenimiento o cambio, la Subdirección de Información debe realizar respaldo de la información y un borrado seguro.
- Para el retiro de activos de las instalaciones de la Unidad se debe tener en cuenta lo establecido en el control SI-A.7.2 Entrada física del presente documento.
- Para el retiro de activos, la Subdirección de Gestión Corporativa deberá llevar un control del inventario con el fin de mantener registro de asignación y devolución.
- Para mantener la seguridad y privacidad de la información en los equipos y activos fuera de las instalaciones de la Unidad y que contengan información clasificada o reservada, estos deben contar con lo establecido en el SI-A.8.24 Uso de criptografía.

Control SI-A.7.10 Medios de almacenamiento

- La Subdirección de Información debe establecer la documentación necesaria para el uso correcto y control de medios removibles.
- Es responsabilidad de cada colaborador tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío de este.
- Se prohíbe el uso de medios removibles que contengan información reservada o clasificada de la Unidad en dispositivos de acceso al público.
- Todo medio removible deberá ser escaneado mediante el antivirus suministrado por la Subdirección de Información cada vez que se conecte a un equipo de la Unidad (para el caso de las áreas que se autorice el uso de dichos medios).
- La Subdirección de Gestión Corporativa debe crear o actualizar si fuere necesario el procedimiento o documento donde se establezca la disposición final de residuos de aparatos eléctricos y electrónicos (RAEE).
- Se deberán emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los medios de propiedad de la Unidad o en servicio de alquiler que serán reutilizados o eliminados y dejar evidencias de la actividad, con el fin de controlar que la información de la entidad contenida en estos medios no se pueda recuperar. Esta solicitud deberá ser mediante requerimiento a la mesa de servicios, con aprobación del jefe inmediato o supervisor de contrato.

Control SI-A.7.11 Servicios públicos de respaldo

- Para propender por la continuidad de los servicios y la operación de la Unidad en caso de fallas en el fluido eléctrico externo, la Subdirección de Gestión Corporativa debe suministrar una planta eléctrica o UPS, y garantizar su manteamiento preventivo y correctivo.
- La Subdirección de Gestión Corporativa debe mantener un listado actualizado con los datos de contacto de emergencia y ponerlos a disposición del personal en caso de interrupción de los servicios públicos.

Control SI-A.7.12 Seguridad del cableado

- La Subdirección de Gestión Corporativa debe proteger el cableado que transporta voz, datos y suministro de energía eléctrica contra la interceptación, interferencia o daños de cualquier tipo dentro del perímetro de la Unidad.

- Los cables de energía eléctrica deberán estar separados de los cables de comunicaciones para evitar interferencia y ruido.
- Al momento de instalar o actualizar el cableado estructurado se debe tener en cuenta las consideraciones técnicas de las normas vigentes y el Reglamento Técnico de Instalaciones Eléctricas RETIE.

Control SI-A.7.13 Mantenimiento de equipos

- La Subdirección de Información debe definir mecanismos de soporte y mantenimiento a los equipos de cómputo, servidores y equipos activos de red de la entidad y debe llevar registro de estos.
- Solo el personal autorizado por la Subdirección de Información puede llevar a cabo el mantenimiento o las reparaciones a los equipos de cómputo y servidores activos de red de la entidad.
- Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deberán ser programadas por la Subdirección de Información y surtir el proceso de gestión de cambios definido por la Unidad.

Control SI-A.7.14 Eliminación segura o reutilización de equipos

Cuando un equipo o medio extraíble sea reasignado o retirado de servicio, la Subdirección de Información debe garantizar la eliminación de toda información mediante mecanismos de borrado seguro teniendo en cuenta que previo a esta actividad debe realizarse una copia de seguridad de esta; en caso de dar de baja para disposición final y no para subastar, se debe tener en cuenta lo establecido en el Control SI-A.5.10 Uso aceptable de la información y otros activos asociados.

6.1.4 Controles de Tecnología

Control SI-A.8.1 Dispositivos finales de usuarios

- Los colaboradores de la Unidad deben bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el equipo de cómputo.
- Los colaboradores de la Unidad que impriman documentos con información clasificada o reservada, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
- No se debe reutilizar documentos impresos con clasificación (Clasificada o Reservada), estos deben ser destruidos.
- La Subdirección de Información debe configurar como política general que todos los equipos de cómputo

que se encuentren en el dominio de la Unidad se les bloquee automáticamente la sesión después de tres (3) minutos de inactividad.

- Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la entidad debe acogerse a la política de “Trae tu propio dispositivo”.

Control SI-A.8.2 Derechos de acceso privilegiado

- La Subdirección de Información debe establecer mecanismos para verificar el monitoreo a las actividades realizadas por los usuarios con accesos privilegiados por lo menos dos (2) veces al año y podrán depurar dichos accesos.
- La Subdirección de Información debe contemplar que los requisitos de autenticación para los derechos de acceso con privilegios deben ser superiores a los requisitos para los derechos de acceso normales (ver Control SI-A.5.18).
- El subdirector de información es quien autorizará y aprobará los derechos de acceso con privilegios. Se deberá llevar un registro de todos los privilegios asignados.
- La Subdirección de Información deberá establecer los requisitos para la expiración de los derechos de acceso privilegiado.
- Las cuentas de usuario por defecto de los sistemas operativos o aplicaciones tales como: “root”, “adm”, “admin”, “administrador”, “SQLAdmin”, “administrator” y “system”, entre otros, deben ser deshabilitadas siempre que no sean de uso obligatorio para el funcionamiento del servicio, de ser así, las credenciales de acceso deben ser asignadas, controladas, monitoreadas y vigiladas por los administradores de los servicios tecnológicos de la Subdirección de Información, éstas deben cumplir con los parámetros definidos para el uso de contraseñas.

Control SI-A.8.3 Restricción de acceso a la información

- La Subdirección de Información debe implementar controles para que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
- La Subdirección de Información debe establecer los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe implementar para los desarrolladores internos o externos acceso limitado y controlado a los datos y archivos que se encuentren en dicho ambiente.
- El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deben estar restringidos y estrictamente controlados.
- Las sesiones inactivas deben cerrarse después de un período de inactividad definido de 3 minutos y se

deben usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.

Control SI-A.8.4 Acceso al código fuente

- El acceso al código fuente del programa es limitado, su acceso y almacenamiento centralizado, solamente será para los ingenieros desarrolladores y de soporte autorizados por la Subdirección de Información. Los desarrolladores no deben tener acceso directo al repositorio de código fuente, sino a través de herramientas de desarrollo que controlan las actividades y autorizaciones en dicho código; se debe mantener un registro de auditoría de todos los accesos y de todos los cambios realizados.
- La actualización y el acceso al código fuente y los elementos asociados se deben realizar de acuerdo con los procedimientos de control de cambios y solo después de recibir la autorización adecuada.
- Las librerías de los sistemas de información no deberán estar contenidas en el ambiente de producción.
- Todo desarrollador que requiera trabajar con los códigos fuentes desde su computador personal adicionalmente deberá tener en cuenta:
    - Tener instalado un antivirus (actualizado) en la máquina.
    - Contar con un sistema operativo actualizado.
    - Contar con cifrado de disco duro el cual envite obtener datos del disco en caso de pérdida o robo.
    - Contar con contraseña de inicio de sesión.
    - Configurar el bloqueo de la sesión posterior a 3 minutos de inactividad.
    - No almacenar histórico de versiones WAR o códigos fuentes dentro de su equipo.

Control SI-A.8.5 Autenticación segura

- La Subdirección de Información debe integrar la autenticación de las aplicaciones con el Directorio Activo.
- La Subdirección de Información debe implementar factores de autenticación adicionales (también conocidos como autenticación de varios factores) para acceder a los componentes de la infraestructura tecnológica de la Unidad, como a los sistemas de información críticos.
- Se deberá proporcionar protección contra intentos de inicio de sesión forzada en nombres de usuario y contraseñas (por ejemplo, mediante CAPTCHA) que requiera el restablecimiento de la contraseña después de un número predefinido de intentos fallidos o que bloquea al usuario después de un número máximo de errores.

Control SI-A.8.6 Gestión de la capacidad

- La Subdirección de Información debe documentar la gestión de capacidad de la plataforma tecnológica, definir su responsable y mantenerla actualizada, la cual permita:
  - Evaluar las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.
  - Monitorear el rendimiento de la infraestructura tecnológica para determinar el uso de la capacidad existente.
  - Analizar los datos de rendimiento y capacidad de la plataforma tecnológica de la Unidad.
  - Definir los acuerdos de niveles de servicio.
  - Asignar los recursos adecuados de hardware y software, para todos los servicios y aplicaciones de tecnología.
- La Subdirección de Información debe documentar las recomendaciones de mejora de la infraestructura de tecnología.
- La Subdirección de Información debe realizar pruebas de esfuerzo de los sistemas y servicios para confirmar que hay suficiente capacidad del sistema para satisfacer los requisitos de rendimiento máximo.
- La Subdirección de Información debe definir los indicadores de monitoreo correspondientes a la gestión de capacidad de la plataforma tecnológica.

Control SI-A.8.7 Protección contra Malware

- La Subdirección de Información debe definir y documentar los controles para la detección, prevención y recuperación contra códigos maliciosos.
- La Subdirección de Información en conjunto con el Oficial de Seguridad y Privacidad de la Información deben realizar campañas de concienciación de usuarios en materia de protección, prevención y recuperación contra códigos maliciosos.
- La Subdirección de Información debe mantener actualizada la base de datos, base de firmas y parches correspondiente del software antivirus y debe asegurar que esta herramienta no pueda ser deshabilitada de los equipos de la Unidad.
- La Subdirección de Información debe dictar los lineamientos para la instalación del software antivirus con el fin de brindar protección contra códigos maliciosos en todos los recursos informáticos de la Unidad.
- La Subdirección de Información debe aplicar las actualizaciones y parches de seguridad de los sistemas operativos de los equipos y servidores de la Unidad para protegerlos contra códigos maliciosos.
- Todo mensaje sospechoso de procedencia desconocida o notificado mediante alertas configuras debe ser inmediatamente reportado a la Subdirección de Información a través de la mesa de servicios,

tomando las medidas de control necesarias.

- La Subdirección de Información debe establecer mecanismos para evidenciar la gestión de las alertas desplegadas en la consola de antivirus validando las acciones tomadas para su solución.

Control SI-A.8.8 Gestión de las vulnerabilidades técnicas

- La Subdirección de Información debe realizar mínimo una vez al año una revisión de vulnerabilidades técnicas a los sistemas de información críticos y misionales por medio de Ethical Hacking y/o pruebas de penetración.
- La Subdirección de Información debe establecer mecanismos para documentar, informar, gestionar y corregir las vulnerabilidades encontradas, adoptando acciones correctivas para mitigar los hallazgos, minimizar el nivel de riesgo y reducir el impacto.
- La Subdirección de Información debe definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, las pruebas de gestión, la aplicación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.
- La Subdirección de Información debe realizar un seguimiento del uso de bibliotecas de terceros y del código fuente en busca de vulnerabilidades. Esto debería ser incluido en la codificación segura.
- Cuando la Unidad utiliza un servicio en la nube proporcionado por un proveedor de servicios, dicho proveedor debe asegurar la gestión de vulnerabilidades técnicas de sus recursos, estas responsabilidades deben hacer parte de los acuerdos de servicios establecidos.

Control SI-A.8.9 Gestión de la configuración

Para la gestión de la configuración la Subdirección de Información debe considerar:

- Que se encuentren documentadas las configuraciones de seguridad, de hardware, de software, de servicios y redes.
- Que se tengan establecidos procesos o herramientas para aplicar las configuraciones definidas.
- Que se tengan establecidas funciones, responsabilidades y procedimientos para garantizar los cambios de esas configuraciones definidas.
- Que se mantenga registro de todos los cambios de configuración. Se tenga una BD de configuraciones.
- Que los cambios en la configuración de seguridad, de hardware, de software, de servicios y redes sean gestionados.
- Que se tengan definidas plantillas estándar para la configuración segura de hardware, software, servicios y redes (minimizar niveles de acceso, deshabilitar identidades, deshabilitar funciones o servicios,

restringir accesos, sincronizar contra el NTP, cambiar información predeterminada).

Control SI-A.8.10 Eliminación de información

- La Unidad debe tener en cuenta aspectos al eliminar información sobre sistemas, aplicaciones y servicios tales como: en la selección de un método de borrado seguro, obtención de pruebas de los resultados de la eliminación, acuerdos establecidos con los proveedores en los que se consideren incluir requisitos sobre la eliminación de información durante y al terminar dichos servicios.
- De acuerdo con el método de eliminación, la Unidad realizará configuración de los sistemas con el fin de destruir la información de forma segura cuando ya no sea necesaria o cuando se haga por solicitud del propietario de esta.
- Se debe realizar eliminación de versiones obsoletas, copias y archivos temporales donde quiera que se encuentren.
- La Subdirección de Información debe usar software de eliminación segura para borrar información de forma permanente. Si lo realiza un proveedor la Subdirección de Información debe realizar el seguimiento y verificación.
- Para los servicios en la nube la entidad debe comprobar si el método de eliminación proporcionado por el proveedor de servicios es aceptable y validar su aplicabilidad.

Control SI-A.8.11 Enmascaramiento de datos

- La Unidad debe limitar la exposición de datos sensibles y la IIP (privacidad y protección de identificación).
- Se debe dar cumplimiento con los requisitos legales estatutario, reglamentarios y contractuales vigentes.
- Se deben utilizar técnicas de pseudoanonimización o anonimización de la IIP (datos personales) (cifrar, anular o eliminar caracteres, números y fechas variables, sustituir o reemplazar valores con su hash).
- Se debe realizar verificación que los datos han sido adecuadamente pseudoanonimizados o anonimizados (no se considera adecuado si una persona puede ser identificada, aunque los datos que pueden identificarla directamente sean anónimos, por la presencia de otros datos que permiten identificarla indirectamente.
- Las técnicas utilizadas para enmascaramiento de IIP deben tener en cuenta: cualquier requisito legal o reglamentario durante el procesamiento o almacenamiento, no conceder a todos los usuarios acceso a todos los datos de IIP (control de acceso, diseño de interfaces específicas o que los datos no sean visibles o autorizados sino a través de usuarios con privilegios específicos), se deben tener acuerdos o

restricciones sobre el uso de los datos IIP procesados.

Control SI-A.8.12 Fuga de datos

- La Unidad debe tener identificada y clasificada la información para protegerla contra fugas.
- La Subdirección de Información debe realizar supervisión de los canales de fuga de datos (correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos de almacenamiento portátiles).
- La Subdirección de Información debe utilizar herramientas para la prevención de fugas de datos para: identificar y supervisar la información confidencial en riesgo de divulgación no autorizada y detectar la divulgación de información confidencial.
- La Subdirección de Información debe realizar acciones para evitar la fuga, como bloquear los usuarios o las transmisiones de red que exponen información confidencial.
- La Subdirección de Información debe implementar tecnología como herramientas de prevención de fugas de datos (DLP).

Control SI-A.8.13 Copias de SI (respaldos)

- La Subdirección de Información debe definir y documentar un plan o procedimiento de copias de respaldo y restauración de la información de la Unidad, donde se establezca el esquema, de qué, cómo, quién, con qué periodicidad, tipo de respaldo, nivel de criticidad y los criterios utilizados para tomar la muestra de la restauración mensual.
- La Subdirección de Información debe definir y documentar lineamientos para la realización de copias de respaldo de:
  - Bases de datos de producción.
  - Software de aplicaciones.
  - Sistemas operativos.
  - Configuraciones de servidores.
  - Software base de la Unidad.
- La Subdirección de Información debe realizar y mantener las copias de respaldo de la información digital solicitadas.
- La Subdirección de Información debe disponer de herramientas tecnológicas para gestionar la información digital y asegurar que estas dispongan de copias de respaldo.
- La Subdirección de Información debe definir mecanismos para la custodia y almacenamiento de las

copias de respaldo, almacenar las copias de seguridad en una ubicación remota segura y a una distancia suficiente para evitar cualquier daño causado por un desastre en el sitio principal.

- La Subdirección de Información debe tener un inventario y bitácora de las copias de respaldo que se realizan y de las copias de respaldo que se restauran.
- La Subdirección de Información debe generar mecanismos que mantengan la integridad y confidencialidad de las copias de respaldo.
- Los colaboradores deben utilizar los repositorios dispuestos por la Subdirección de Información para almacenar la información de la Unidad, dado que estos cuentan con políticas de copias de seguridad configuras automáticamente.
- La Subdirección de Información debe probar regularmente los medios de copia de seguridad para asegurar que se pueden confiar en ellos para su uso de emergencia cuando sea necesario.
- Los colaboradores son responsables de la información que resida en el equipo asignado y serán los encargados de mantener las copias de respaldo de sus archivos, y la información debe ser entregada al supervisor del contrato o jefe inmediato al finalizar su vinculación con la Unidad.
- Para el uso de servicios en la nube, la Subdirección de Información debe realizar copias de seguridad de las aplicaciones y los sistemas en el entorno de dicho servicio. La Subdirección de Información debe determinar si se cumplen los requisitos de copias de seguridad en estos ambientes de nube.
- La Subdirección de Gestión Corporativa (Gestión Documental) debe determinar el período de retención de la información esencial de la entidad, tomando en consideración cualquier requisito de retención de copias archivadas. Se debería considerar la eliminación de información en los medios de almacenamiento utilizados para las copias de seguridad una vez que el período de retención de la información expire, teniendo en cuenta la legislación y las regulaciones vigentes.

Control SI-A.8.14 Redundancia de las instalaciones de procesamiento de información.

- La Subdirección de Información, deben implementar redundancia suficiente, para lo cual deberá considerar componentes o arquitecturas redundantes, teniendo en cuenta las necesidades de los procesos de la entidad.
- La Subdirección de Información debe probar los componentes o arquitecturas redundantes implementadas para asegurar que después de una falla el componente funcione.

Control SI-A.8.15 Registros

- La Subdirección de Información debe generar registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren.

- La Subdirección de Información debe salvaguardar los registros de auditoría que se generen de cada sistema.
- La Subdirección de Información puede utilizar una herramienta SIEM o un servicio equivalente para almacenar, correlacionar, normalizar y analizar la información de registro, así como para generar alertas.

Control SI-A.8.16 Actividades de monitoreo

- La Subdirección de Información debe monitorear las excepciones o los eventos de seguridad de la información.
- La Subdirección de Información debe monitorear la infraestructura tecnológica para verificar que los usuarios sólo la usen para actividades propias de su labor y de la misión de la entidad y atender cualquier alerta que se genere.
- La Subdirección de Información debe monitorear, identificar e informar sobre las transferencias de grandes volúmenes de información por fuera del dominio, con el fin de prevenir fugas de información.
- Los responsables técnicos de los sistemas de información, base de datos, equipos de infraestructura tecnológica, deben propender porque los mismos tengan activados o implementados sus logs de auditoría a fin de evidenciar fallas o cambios no autorizados.

Control SI-A.8.17 sincronización de relojes

La Subdirección de Información debe sincronizar los relojes de los servidores con una única fuente de referencia de tiempo (http://horalegal.inm.gov.co/), con el fin de garantizar la exactitud de los registros de auditoría.

Control SI-A.8.18 Uso de programas utilitarios privilegiados

- La Subdirección de Información debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información, no tengan instalados en sus equipos de cómputo programas utilitarios que permitan escalar privilegios o evadir controles de seguridad informáticos sin ser debidamente autorizados.
- La Subdirección de Información debe monitorear a los administradores de los recursos tecnológicos y servicios de red, para que no hagan uso de programas utilitarios que permitan acceso a los sistemas operativos, firmware o conexión a las bases de datos para anular la seguridad de los sistemas de información alojados sobre la plataforma tecnológica.
- La Subdirección de Información debe generar y mantener actualizado un listado de programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información autorizados.

- La Subdirección de Información debe retirar o deshabilitar los programas utilitarios privilegiados no autorizados de la plataforma tecnológica, los servicios de red y sistemas de información y bloquear su conexión a través de los servicios perimetrales e internos de seguridad informática.

Control SI-A.8.19 instalación de software en los sistemas operativos

- La Subdirección de Información debe controlar y tener registros de la actualización del software en producción, aplicaciones y librerías de programas propios de la Unidad.
- La Subdirección de Información debe conservar las versiones anteriores del software de aplicación como una medida de contingencia.
- La Subdirección de Información debe usar controles para proteger todo el software implementado y la documentación del sistema.
- La Subdirección de Información debe probar y evaluar la aplicación de actualizaciones antes de su instalación y valorar los riesgos asociados, para asegurar que son eficaces y no producen efectos secundarios.
- La Subdirección de Información debe restringir a los usuarios finales la instalación de software en los equipos de la Unidad.
- La Subdirección de Información debe establecer y monitorear que la infraestructura tecnológica sea usada exclusivamente para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas, y atender cualquier alerta que se genere.
- La Subdirección de Información debe controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada y no viole los derechos de autor.
- La Subdirección de Información debe realizar de manera periódica una inspección del software instalado en los equipos de la Unidad y debe desinstalar el software no autorizado.
- La Subdirección de Información es la responsable de instalar, configurar y dar soporte a los equipos de la Unidad.
- Sólo está permitido el uso de software licenciado por la Unidad y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado por la Subdirección de Información.
- Las aplicaciones generadas por la Unidad en desarrollo de su misión institucional deben ser reportadas a la Subdirección de Información para su administración.
- La Subdirección de Información es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales y comerciales.
- El software de código abierto utilizado en los sistemas operativos debe mantenerse en la última versión apropiada del software.

- La Subdirección de Información debe contemplar el principio de privilegio mínimo en la instalación de software en sistemas operativos.

Control SI-A.8.20 Seguridad de las redes

- La Subdirección de Información debe mantener documentación actualizada, incluidos diagramas de red y archivos de configuración de dispositivos (por ejemplo, routers, switches).
- La Subdirección de Información debe adoptar el protocolo IPv6 con base en las características de Confidencialidad, Integridad, Disponibilidad y Privacidad de la información; a fin de generar mecanismos de direccionamiento IP de acceso seguro y uso eficiente de las infraestructuras de información y comunicación de la entidad.
- La Subdirección de Información debe disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones de la Unidad.
- Se deben diseñar redes perimetrales con los siguientes objetivos:
  - No se pueden hacer consultas directas a la red interna de la Unidad desde redes externas e internet.
  - Se deberá realizar la segmentación de redes y listas de acceso a los servicios de la Unidad tales como servidores y administración de la infraestructura tecnológica.
- El acceso a la red de datos de la Unidad y a los sistemas de información soportados por la misma, es de carácter restringido. Se deben conceder permisos con base a “la necesidad de conocer” y el “acceso mínimo requerido” conforme a los criterios de seguridad de la información contemplados en la presente política.

Control SI-A.8.21 Seguridad de los servicios de red

- La Subdirección de Información es la responsable de garantizar que los puertos físicos y lógicos de diagnósticos y configuración de plataformas que soporten sistemas de información deban ser seguros y estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.
- La Subdirección de Información debe establecer la documentación necesaria para el uso de los servicios de red y aplicaciones.
- La Subdirección de Información debe realizar revisiones y monitoreo regularmente a la gestión de los servicios para validar que se encuentran en los acuerdos de servicios de red establecidos con los proveedores.
- La Subdirección de Información debe definir controles para la transferencia de información a través de redes públicas para las aplicaciones de la Unidad.

Control SI-A.8.22 Segregación de las redes

- La Subdirección de Información debe proporcionar una plataforma tecnológica que soporte los sistemas de información, esta debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad.
- La Subdirección de Información debe realizar segmentación de redes para colaboradores y visitantes de la Unidad.
- La Subdirección de Información debe establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

Control SI-A.8.23 Filtrado web

- La Subdirección de Información debe identificar las categorías de sitios web a los que el personal de la Unidad debería o no tener acceso.
- La Subdirección de Información debe establecer reglas para un uso seguro y apropiado de recursos en línea, incluida cualquier restricción a sitios web indeseables o inadecuados y aplicaciones basadas en web.
- La Subdirección de Información debe impartir sensibilizaciones al personal sobre el uso seguro y adecuado de los recursos en línea, incluido el acceso a la web.

Control SI-A.8.24 Uso de criptografía

- La Subdirección de Información debe establecer los controles criptográficos en los siguientes casos:
  - Para la protección de claves de acceso a sistemas.
  - Para la información digital reservada y clasificada.
  - Para el envío de correo electrónico con información reservada y clasificada.
  - En los canales digitales oficiales de recepción de solicitudes, peticiones y de información, dispuestos en la sede electrónica de la Unidad.
- La Subdirección de Información debe verificar que todo sistema de información que requiera realizar transmisión de información clasificada o reservada cuente con mecanismos de cifrado de datos.
- La Subdirección de Información debe desarrollar, establecer e implementar estándares para la aplicación de controles criptográficos en los datos y servicios que lo requieran por su criticidad.
- La Subdirección de Información debe utilizar controles criptográficos para la transmisión de información

clasificada o reservada, fuera de la Unidad.

- La Subdirección de Información debe asegurar que los controles criptográficos de los sistemas de información construidos cumplan con los estándares establecidos.
- La Subdirección de Información debe disponer de herramientas que permitan el cifrado de medios de almacenamiento de información.
- La Subdirección de Información debe proveer a los usuarios de la Unidad los métodos de cifrado de la información, así como administrar el software o herramienta utilizado para tal fin, y poner a disposición la guía para el usuario.
- La Subdirección de Información debe establecer mecanismos para la gestión de llaves criptográficas donde se evidencie el ciclo desde su creación hasta el retiro y destrucción.

Control SI-A.8.25 Ciclo de vida de desarrollo seguro

- La Subdirección de Información debe establecer los mecanismos necesarios para la creación de software, teniendo en cuenta los siguientes aspectos:
  - Orientar sobre buenas prácticas de seguridad en el desarrollo del software.
  - Requisitos de seguridad en el control de versiones.
  - Capacidad de los desarrolladores para evitar, encontrar y resolver vulnerabilidades.
- La Subdirección de Información debe tener en cuenta el punto anterior para la reutilización de códigos.
- La Subdirección de Información debe proteger los códigos ejecutables y código de desarrollo o compiladores del software operacional y aplicaciones propias de la Unidad.

Control SI-A.8.26 Requisitos de seguridad de la información de las aplicaciones

- Los requisitos de seguridad y privacidad de la información y seguridad digital de las aplicaciones serán determinados a través de una evaluación de riesgos, con el apoyo del oficial de seguridad y privacidad de la información.
- La Subdirección de Información debe disponer de requerimientos para las solicitudes de nuevos sistemas de información o modificaciones a los existentes en la Unidad que cuenten con el análisis e implementación de criterios de seguridad del software.
- La Subdirección de Información debe contar con mecanismos para justificar, acordar y documentar en la fase de requisitos y en la fase de modificación de los sistemas de la Unidad, los criterios de seguridad y privacidad de la información y seguridad digital.
- La Subdirección de Información debe contar con los siguientes criterios adicionales de seguridad y privacidad de la información y seguridad digital:

- Suministro de acceso y de autorización para usuarios de la Unidad, al igual que para usuarios privilegiados o técnicos.
- Informar a los usuarios y operadores sobre sus deberes y responsabilidades.
- Requisitos derivados de los procesos como registro de transacciones, seguimiento y no repudio.
- Protección frente a ataques malintencionados o interrupciones no intencionadas.
- Requisitos legales, estatutarios y reglamentarios en la jurisdicción donde se genera, procesa, completa o almacena la transacción.

- La Subdirección de Información debe disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones de la Unidad, teniendo en cuenta los siguientes criterios:
  - Contar con información de autenticación secreta de usuario.
  - Mantener la privacidad en las partes involucradas.
  - Cifrar las comunicaciones cuando sea necesario.
  - Asegurar los protocolos de comunicación.
  - La información almacenada de las transacciones no se encuentre pública.

Control SI-A.8.27 Principios de arquitectura e ingeniería de sistemas seguros

La Subdirección de Información debe definir ambientes de desarrollo seguro, teniendo en cuenta los siguientes aspectos:

- El carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir.
- Requisitos externos como reglamentaciones o políticas.
- Controles de seguridad y privacidad ya establecidos por la Unidad.
- Control de acceso al ambiente de desarrollo.
- Seguimiento de los cambios en el ambiente de desarrollo y los códigos almacenados en este.
- Control sobre el movimiento de datos desde y hacia el ambiente de desarrollo.

- La Subdirección de Información debe documentar el desarrollo de sistemas de información basado en los principios de seguridad.
- La Subdirección de Información debe realizar verificación periódica a la documentación de los sistemas de información en relación con los estándares de seguridad que hayan surgido y amenazas potenciales.

Control SI-A.8.28 Codificación segura

- La Subdirección de Información antes de la codificación deberá contemplar el diseño y arquitectura seguros, incluida la modelización de amenazas, adicionalmente, deberá obligatoriamente tener en cuenta normas y metodologías de codificación segura.

- La Subdirección de Información debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deberán contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
- Los desarrolladores deberán asegurar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- Los desarrolladores deberán establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
- Los desarrolladores deberán asegurar que no se desplieguen en la pantalla las contraseñas ingresadas, así como deberán deshabilitar la funcionalidad de recordar campos de contraseñas.
- Los desarrolladores deberán asegurar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- Los desarrolladores deberán asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deberán tener un periodo de validez establecido; se deberá forzar el cambio de las contraseñas temporales después de su utilización.
- Los desarrolladores deberán establecer que periódicamente se valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.
- Lo desarrolladores deberán documentar el código y eliminar los defectos de programación, que pueden permitir la explotación de las vulnerabilidades de la seguridad y privacidad de la información y seguridad digital.
- La Subdirección de Información debe aplicar actualizaciones de forma segura a las aplicaciones de la Unidad, dichas actualizaciones deberán realizare de forma periódica o en el momento en que se requiera.

Control SI-A.8.29 Pruebas de seguridad en el desarrollo y la aceptación

- La Subdirección de Información debe contemplar en los cambios y en los nuevos sistemas de información, pruebas asociadas a seguridad y privacidad de la información y seguridad digital, dichas pruebas de seguridad deberán incluir pruebas de:
    - Funciones de seguridad, por ejemplo, autenticación de usuarios, restricción de acceso y uso de cifrado.
    - Codificación segura.
    - Configuraciones seguras, incluidas las de los sistemas operativos, firewall y otros componentes de seguridad.
- La Subdirección de Información debe contar en sus pruebas de aceptación de sistemas de información

requisitos de seguridad y privacidad de la Información y seguridad digital.

- En el caso de los componentes de desarrollo y compra subcontratados, debería seguirse un proceso de adquisición. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados. Los productos y servicios deberían ser evaluados según estos criterios antes de su adquisición.

Control SI-A.8.30 Desarrollo subcontratado

La Subdirección de Información debe definir controles para que los sistemas adquiridos externamente cumplan con los siguientes aspectos:

- Acuerdos de licenciamiento, sucesión de derechos patrimoniales, propiedad de códigos y derechos de propiedad intelectual relacionados con el sistema de información contratado externamente.
- Requisitos contractuales para prácticas seguras de desarrollo, diseño, codificación y pruebas.
- Evidencia del uso de umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
- Evidencia de pruebas de seguridad para vigilar que no exista contenido malicioso intencional y no intencional en el momento de la entrega.
- Evidencia de pruebas para proteger contra la presencia de vulnerabilidades conocidas.
- Derecho contractual con relación a procesos y controles de desarrollo de auditorías.
- Documentación del ambiente de construcción usado para crear entregables.
- La legislación aplicable, por ejemplo, sobre protección de datos personales.

Control SI-A.8.31 Separación de ambientes de desarrollo, pruebas y producción

- La Subdirección de Información debe propender por la separación de los ambientes de desarrollo, pruebas y producción, los cuales deben estar separados de manera física y lógica.
- La Subdirección de Información debe definir, documentar y aplicar lineamientos seguros para la transferencia entre ambientes.
- La Subdirección de Información debe utilizar en los ambientes de prueba, datos que no sean sensibles para la Unidad o utilizar herramientas o técnicas para ofuscar, anonimizar o enmascarar los datos.
- La Subdirección de Información debe permitir que los ambientes de prueba, desarrollo y producción sean similares para prevenir situaciones en las cuales el software desarrollado presente comportamientos distintos y errores.
- La Subdirección de Información debe utilizar nombres de dominios diferentes para los ambientes de prueba, desarrollo y producción para evitar confusión y diferenciar de manera clara cada ambiente.
- La Subdirección de Información debe garantizar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y nunca en los ambientes de pruebas o producción.

Control SI-A.8.32 Gestión de cambios

- La Subdirección de Información debe establecer la documentación necesaria que permitan asegurar la gestión de cambios normales y de emergencia a nivel de infraestructura, aplicativos y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficiencia, seguridad, calidad y permitan determinar las actividades y responsables en la gestión de cambios.
- La Subdirección de Información debe establecer un comité de cambios normales y de emergencia, quien se encargará de evaluar, aprobar o negar la implementación de los cambios.
- La Subdirección de Información debe establecer la documentación necesaria que contenga el detalle de la operación de gestión de cambios normales y de emergencia.
- La Subdirección de Información debe definir controles para que los cambios en los sistemas de información de la Unidad sean documentados, teniendo en cuenta la integridad de los sistemas desde las primeras etapas de diseño y a través de los mantenimientos posteriores.
- La Subdirección de Información debe definir un proceso formal para la inclusión y cambios importantes en los sistemas de información involucrando pruebas, control de calidad e implementación.
- La Subdirección de Información debe definir para los cambios en los sistemas de la Unidad los siguientes aspectos:
  - Niveles de autorización acordados.
  - Presentar los cambios a los usuarios autorizados.
  - Revisar la integridad para asegurar que no se vean comprometidos los cambios.
  - Identificar y validar el código crítico de seguridad.
  - Antes de cualquier cambio, se debe asegurar que los usuarios autorizados aceptan los cambios.
  - Mantener un control de versiones para las actualizaciones de los sistemas.
  - Mantener un rastro de auditoría de los cambios.
  - Se debe asegurar que los cambios se hagan en momentos adecuados y que no afecten los procesos de la Unidad.
- La Subdirección de Información debe guardar en un repositorio, las versiones anteriores de cada sistema de información que es actualizado.
- La Subdirección de Información debe definir la manera de revisar después de un cambio importante que el sistema de información alterado no se haya comprometido.
- La Subdirección de Información debe definir la manera para notificar a tiempo los cambios de los sistemas, permitiendo realizar pruebas y revisiones apropiadas antes de su implementación.
- La Subdirección de Información debe evitar las modificaciones a los paquetes de software, en la medida de lo posible se deberán usar directamente los suministrados por el proveedor; limitándose únicamente a cambios necesarios. Cuando se hagan, se deberán tener en cuenta los siguientes aspectos:

- El riesgo en que se puede ver involucrado el sistema de información.
- Verificar si se requiere consentimiento del proveedor.
- Verificar la posibilidad que el proveedor realice dichos cambios.
- El impacto en dado caso que el mantenimiento futuro recaiga en manos de la Unidad.
- La compatibilidad con otro software en uso.
- Se debe conservar el software original cuando se hayan realizado cambios en los paquetes de este.

Control SI-A.8.33 Información para las pruebas

- La Subdirección de Información debe utilizar herramientas o técnicas para ofuscar, anonimizar o enmascarar los datos o evitar durante la ejecución de pruebas en ambientes de desarrollo el uso de datos que contengan información personal o información sensible de la Unidad que esté contenida en el ambiente de producción de las aplicaciones.
- La Subdirección de Información debe tener en cuenta controles de acceso a los ambientes de producción y de prueba.

Control SI-A.8.34 Protección de los sistemas de información durante las pruebas de auditoría

- El asesor de control interno de acuerdo con el PAAI (Programa Anual de Auditoría Interna) ejecutará auditorías a los sistemas de información críticos en producción cuando se encuentren contemplados en la planeación y para ello tendrá acceso limitado a los datos en modo de solo consulta.
- El asesor de control interno debe mantener los documentos, dispositivos y medios utilizados para las auditorias de los sistemas de información custodiados de accesos no autorizados.
- El asesor de control interno debe documentar los resultados de las auditorias de los sistemas de Información de la Unidad.

Control SI-A.8.35 Seguridad de la información en la sede electrónica

- La Subdirección de Gestión Corporativa con el apoyo de la Subdirección de Información y el Oficial de Seguridad y Privacidad de la Información, deben definir los lineamientos de la implementación de la sede electrónica de la Unidad Administrativa Especial de Alimentación Escolar - Alimentos para Aprender, en donde se deberán integrar todos los portales, sitios web, plataformas, ventanillas únicas, aplicaciones y soluciones existentes.

- La Subdirección de Gestión Corporativa debe identificar los canales digitales oficiales de recepción de solicitudes, peticiones y de información, y la Subdirección de Información debe implementar los mecanismos de cifrado de información para dichos canales.
- La Subdirección de Gestión Corporativa con el apoyo de la Subdirección de Información, deberán implementar un sistema de gestión documental electrónica y de archivo digital, asegurando la conformación de expedientes electrónicos con características de integridad, disponibilidad y autenticidad de la información. Adicionalmente, para la emisión, recepción y gestión de comunicaciones oficiales, a través de los diversos canales electrónicos, deberá asegurar un adecuado tratamiento archivístico.
- La Subdirección de Gestión Corporativa junto con el apoyo de la Subdirección de Información y el Oficial de Seguridad y Privacidad de la Información , deben establecer las estrategias que permitan el tratamiento adecuado de los documentos electrónicos y garantizar la confidencialidad, integridad, disponibilidad y acceso a largo plazo conforme a los principios y procesos archivísticos definidos por el Archivo General de la Nación en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Las dependencias responsables de trámites, procesos y procedimientos dirigidos a los ciudadanos deberán implementar los lineamientos de la sede electrónica definidos por la entidad en concordancia con las medidas jurídicas, organizativas y técnicas que garanticen la calidad, seguridad, privacidad, disponibilidad, integridad, confidencialidad, accesibilidad, neutralidad e interoperabilidad de la información y de los servicios.
- La sede electrónica debe cumplir con los lineamientos de seguridad (Anexo 3) establecidos en la Resolución 1519 de 2020 por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

Código: SI-A.8.36 Seguridad de la Información para el SIIF NACIÓN

- El Oficial de Seguridad y Privacidad de la Información, la Subdirección de Información y la Subdirección de Gestión Corporativa deben documentar los lineamientos para el manejo y control de los recursos tecnológicos utilizados para la administración y gestión financiera de la Unidad Administrativa Especial de Alimentación Escolar - Alimentos para Aprender.
- Toda la información del SIIF Nación debe ser protegida contra acceso no autorizado para mantener su confidencialidad, integridad, disponibilidad y privacidad.
- Cumplir con los requerimientos mínimos en seguridad y privacidad de la información e informática en los equipos utilizados para la realización de transacciones financieras.

- Para acceder al SIIF Nación se deben definir usuarios, roles y perfiles los cuales deben ser tramitados de acuerdo con lo establecido por la Administración del SIIF Nación y la Unidad Administrativa Especial de Alimentación Escolar - Alimentos para Aprender.

Se debe dar cumplimiento a lo establecido en las políticas de seguridad de la información del SIIF Nación, establecidas por el Ministerio de Hacienda y Crédito Público, que se encuentren vigentes.

CONTROL DE CAMBIOS

<table>
<tr><th>VERSIÓN</th><th>DESCRIPCIÓN DEL CAMBIO O JUSTIFICACIÓN</th><th>FECHA DE CAMBIO</th></tr>
<tr><td>0</td><td>Se migra el documento a partir del nuevo mapa de procesos aprobado en el Comité Institucional de Gestión y Desempeño del 14 de abril de 2025. Para efectos de trazabilidad, los responsables de la versión migrada de fecha 06/07/2023 fueron los siguientes:

<table>
<tr><th>ELABORÓ</th><th>REVISÓ</th><th>APROBÓ</th></tr>
<tr><td>Sergio Andrés Ramos Pahuana</td><td>Gustavo Adolfo Grisales</td><td>Gustavo Adolfo Grisales</td></tr>
<tr><td>Cargo: Contratista Subdirección de Información</td><td>Cargo: Subdirector Técnico de Información</td><td>Cargo: Subdirector Técnico de Información</td></tr>
<tr><td>Fecha: 29/06/2023</td><td>Fecha: 29/06/2023</td><td>Fecha: 06/07/2023</td></tr>
</table>

Este documento en el marco del anterior mapa de procesos se encontraba codificado como GTI-MN-02</td><td>23/05/2025</td></tr>
<tr><td>1</td><td>Los controles son alineados con la versión 2022 de la norma ISO 27001 Se ajusta la estructura del documento de acuerdo con los dominios contenidos en el Anexo de la norma ISO 27001:2022. Se genera relación de necesidad de desarrollo de formato para seguimiento de implementación de controles de seguridad.</td><td></td></tr>
</table>

ELABORÓ	REVISÓ	APROBÓ
Sergio Andrés Ramos Pahuana	Diego Fernando Salgado Castro	Diego Fernando Salgado Castro
Cargo: Contratista Subdirección de Información	**Cargo:** Subdirector Técnico de Información	**Cargo:** Subdirector Técnico de Información
Fecha: 04/07/2025	**Fecha:** 17/07/2025	**Fecha:** 17/07/2025