LINEAMIENTOS Y DIRECTRICES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021

PROCESO: GESTIÓN DE LA INFORMACIÓN

UNIDAD ADMINISTRATIVA ESPECIAL DE ALIMENTACIÓN ESCOLAR

BOGOTÁ D.C, FEBRERO 2021

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Dentro del marco de las Políticas de Seguridad y Privacidad de la información y la Protección de Datos Personales de la **Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender** (en adelante UApA), se presentan los lineamientos y directrices necesarios para el normal desarrollo de las actividades, tanto de los colaboradores de la UApA como de los terceros involucrados con la misionalidad de la Unidad, con el fin de garantizar la disponibilidad, integridad y confidencialidad de la Información.

La definición e implementación de políticas, metodologías, directrices y recomendaciones basadas en estándares y mejores prácticas, todas orientadas con procesos de TI, fortalecerán los procesos de negocio y garantizarán el aprovechamiento de los recursos informáticos en la Entidad. Así mismo, se facilitará la incorporación y uso efectivo de las tecnologías emergentes de última generación, se aprovecharán mejor las herramientas informáticas y demás servicios de TI requeridos para la integración y el intercambio de la información.

En tal sentido, la Subdirección de Información está consolidando la gestión tecnológica de la Unidad, mediante la definición de los principios, políticas y lineamentos de las diferentes líneas de acción de TI, buscando que se genere un valor agregado sobre las actividades de los usuarios la Entidad. Ahora bien, el mapa de ruta para la definición, estructuración e implementación, parte de la alineación con los objetivos estratégicos establecidos por la UApA en su plan estratégico sectorial y atendiendo los lineamientos propuestos para el desarrollo educativo. De esta manera, una Institucionalidad moderna y tecnificada genera acciones transversales sobre los pilares de la Unidad, al igual que garantiza el cumplimiento a las políticas establecidas por el Departamento Administrativo de la Función Pública para el mejoramiento de la Gestión y el Desempeño de la institucionalidad del Sector.

En razón de lo anterior y considerando la necesidad de incorporar estrategias y controles en el ámbito de las Tecnologías de la Información y las Comunicaciones (en adelante TI), necesarias para el cumplimiento de las metas institucionales, se hace indispensable trazar y comprometer la implementación de la política de gestión de seguridad de la información y protección de datos, la cual proporcione un marco de confianza en el ejercicio de sus deberes con la institucionalidad, el estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Unidad.

En ese sentido y de acuerdo con los principios de tecnología adoptados por la Unidad, con el fin de mantener un control eficiente de las tecnologías de información y comunicaciones aportando valor a la Entidad, se estructura el presente documento de Lineamientos de la Política de Seguridad y privacidad de la Información.

El respectivo contenido y sus actualizaciones serán informados a directivos, funcionarios, contratistas, proveedores, colaboradores y terceros que presten sus servicios o tengan alguna relación con la Unidad, a través de la Dirección General o su delegado y se publicarán en la Intranet.

2. MARCO NORMATIVO

El Estado colombiano cuenta con normatividad vigente que obliga al adecuado tratamiento de la información manejada por las entidades del estado en términos de confidencialidad, integridad y disponibilidad. Teniendo en cuenta lo anterior, la Subdirección de Información emprenderá acciones orientadas a la gestión y protección de la información, en el marco del Plan de acción y del Sistema Integrado de Gestión.

Entre los documentos de referencia se citan:

- **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 1221 del 2008.** Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- **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.
- **Resolución 2999 del 2008.** Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.

- **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 1341 de 2009.** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones.

- **Ley 1437 de 2011.** Capítulo IV, “utilización de medios electrónicos en el procedimiento 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.

- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.

- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.

- **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 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.

- **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.

- **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 1078 de 2015.** Por medio del cual se expide el Decreto Único reglamentario del Sector de Tecnologías de la Información y las comunicaciones.

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

- **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.

- **Ley 2015 de 2018.** Por la cual se modifica la Ley 23 de 2082 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

- **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.

- **Ley 2052 de 2020.** Por medio de la cual se expide el código general disciplinario

- **Ley 2055 de 2020.** Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. “Pacto por Colombia, Pacto por la Equidad”.

3. GLOSARIO

- **Activo de Información:** Es todo aquello que en la entidad es considerado importante o de alta validez para la misma, ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.
- **Carpetas Compartidas:** es igual que una carpeta normal salvo que su contenido será accesible para todos los usuarios que pertenezcan a un mismo grupo de trabajo.
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Copias de respaldo:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Disponibilidad:** Acceso y uso de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **File Server:** Es un servidor de archivos que almacena y distribuye diferentes tipos de archivos informáticos confidenciales o críticos.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Información confidencial o crítica:** Es aquella información que no se debe circular más allá de las personas que están autorizadas a conocerlas en la UApA.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Mesa de Ayuda de Tecnologia:** es el único Centro de Atención al Usuario en donde la OTIS presenta servicios con la posibilidad de gestionar la atención de requerimientos relacionados con los servios TICs en la UApA
- **MSPI:** Es el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información – MINTIC.

- **OneDrive:** Sitio para almacenamiento virtual en la nube de la información pública de las áreas de la institución
- **PAE - Programa de Alimentación Escolar**: El Programa de Alimentación Escolar consiste en el suministro organizado de un complemento nutricional con alimentos, a los niños, niñas y adolescentes matriculados en el sistema educativo público, y el desarrollo de un conjunto de acciones alimentarias, nutricionales, de salud y de formación, que contribuyen a mejorar el desempeño de los escolares y apoyar su vinculación y permanencia en el sistema educativo.
- **PETI**: Plan Estratégico de Tecnologías de la Información y las Comunicaciones.
- **POLÍTICA:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **SDI:** Subdirección de Información de la UApA.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **SGSI**: Sistema de Gestión de Seguridad de la Información.
- **SharePoint:** Sitio para almacenamiento de la información pública para uso interno de la institución.
- **TIC**: Tecnologías de la Información y las Comunicaciones.
- **UApA:** Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender.
- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

4. OBJETIVO

Definir y socializar los lineamientos y directrices que se requieren para garantizar la protección de la información de la UApA, velando por el cumplimiento de la integridad, disponibilidad y confidencialidad de esta.

5. ALCANCE

Los presentes limeamientos y directrices deberán ser cumplidos por todos los colaboradores (contratistas) y terceros de todos los procesos de la UApA y, adicionalmente, por los ciudadanos, persona naturales o jurídicas, nacionales o extranjera que sin tener relación laboral o contractual con la UApA tengan acceso a sus instalaciones y/o servicios tecnológicos.

Propender que los servicios tecnológicos y de comunicaciones se ofrezcan con calidad, confiabilidad, confidencialidad, integridad, disponibilidad y eficiencia, optimizando y priorizando su uso para asegurar su correcta funcionalidad, brindando un nivel de seguridad óptimo que permitan:

- Evitar la materialización de los riesgos identificados.
- Cumplimiento legal y normativo.
- Disminuir las amenazas a la seguridad de la información y los datos.
- Evitar el comportamiento inescrupuloso y uso indiscriminado de los recursos.
- Cuidar y proteger los recursos tecnológicos de la UApA
- Concientizar a la comunidad sobre la importancia del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.

6. LINEAMIENTOS Y DIRECTRICES

6.1 Roles y Responsabilidades

➢ Hacer buen uso de la información que es generada resultado de las actividades laborales.

➢ Almacenar la información resultado del ejercicio de las funciones en la carpeta local o servidor de archivos designado por la Subdirección de Información, de esta forma la SDI podrá grantizár las copias de respaldo, de lo contrario no queda dentro de los presentes lineamientos.

➢ En ninguna circunstancia se podrá divulgar la información clasificada como CONFIDENCIAL o RESERVADA a personas no autorizadas o en espacios públicos o privados. Esta restricción se debe cumplir inclusive después de la terminación del vínculo

laboral y contractual y debe estar incluida en los Acuerdos de Confidencialidad establecidos por la Entidad.

➢ Todos los activos de información del deben tener un propietario, custodio y deben estar debidamente identificados.

➢ Los propietarios de los activos de información son los responsables de aplicar y velar por el cumplimiento de los controles que garanticen la disponibilidad, confidencialidad e integridad de la información de los activos.

➢ Se deben definir e incluir los roles y privilegios de la plataforma tecnológica y sistemas de información, con el fin de crear el procedimiento de solicitud, modificación, eliminación y/o inactivación de usuarios privilegiados.

➢ Se debe seguir el procedimiento de gestión de accesos definido por la SDI.

➢ Todas las solicitudes deben tener fecha de finalización y cuando sean roles que no se encuentren definidos se consideran como privilegios temporales.

➢ La mesa de servicios designada para tal fin debe informar a través de los mecanismos de comunicación seleccionados, que el usuario fue creado y que fueron asignados los privilegios solicitados.

➢ Se debe capacitar a todos los Colaboradores y terceros solicitantes de accesos a componentes tecnológicos y sistemas de información sobre el uso y la responsabilidad que tienen al ser autorizados.

➢ Se debe definir una matriz de roles y responsabilidades en seguridad de la información, la cual debe ser actualizada periódicamente o cada vez que se requiera.

6.2 Gestión Humana: Seguridad

Garantizar la protección de la disponibilidad, integridad y confidencialidad de la información del personal que trabaja en la UApA, a través de mecanismos de validación y concientización del recurso humano que hará uso de esta.

6.2.1. Incorporación de la Seguridad en la matriz de Cargos de la entidad

Deben ser incorporadas los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros.

6.2.2. Control y Política del Personal

Se deben definir controles de verificación del personal en el momento en que se postula al cargo. Estos controles incluirán todos los aspectos legales y de procedimiento que dicta el proceso de contratación de colaboradores de la Unidad.

6.2.3. Acuerdo de Confidencialidad

Todos los Colaboradores y Terceros que ingresen a trabajar en la UApA, deben firmar como parte de sus términos y condiciones iniciales de trabajo, un Acuerdo de Confidencialidad o no divulgación, en caso de que no estuviere incluido como una cláusula dentro del contrato de prestación de servicios o en el Acta de Posesión del funcionario. Este acuerdo debe incluir la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información, el tratamiento de la información de la entidad, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013. Este documento debe ser archivado de forma segura por el área de Talento Humano y Contractual, según sea el caso.

Dentro del mismo acuerdo el Colaborador o Tercero declaran conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violarel derecho a la privacidad ni los derechos del colaborador o tercero.

6.2.4. Selección de personal

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes, de acuerdo con la reglamentación.

Se deben aplicar los controles establecidos por la UApA para otorgar el acceso a la información CONFIDENCIAL o RESERVADA por parte del personal que resulte vinculado a la Entidad.

El área de Talento humano y Contratación son los responsables de realizar la verificación de antecedentes disciplinarios, fiscales y judiciales y que se anexe la documentación requerida para la contratación.

6.2.5. Términos y condiciones Laborales

Todos los Colaboradores y Terceros de la Unidad deben dar cumplimiento a las políticas y normatividad establecida en seguridad y privacidad de la información y debe ser parte integral de los contratos o documentos de vinculación a que haya lugar.

Todos los Colaboradores y Terceros, durante el proceso de vinculación a la UApA, deberán recibir una inducción sobre las Políticas y Lineamientos de Seguridad y Privacidad de la Información.

6.2.6. Entrenamiento, concientización y capacitación

Todos los Colaboradores y Terceros de la UApA deben ser entrenados y capacitados para las funciones, actividades y cargos que van a desempeñar, esto con el fin de sensibilizar a los usuarios sobre la protección adecuada de los recursos y la información de la Entidad. Así mismo, se debe garantizar la comprensión del alcance y contenido de las políticas lineamientos y directrices de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente e integral desde su función.

6.2.7. Formación y Capacitación en Materia de Seguridad de la Información

Todos los colaboradores y terceros cuando sea el caso, que trabajan para la Unidad deben recibir una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos de Seguridad y privacidad de la Información. Dentro del contenido se deben contemplar los requerimientos de seguridad y las responsabilidades legales, así como la capacitación sobre el uso adecuado de las instalaciones de procesamientos de información y los recursos tecnológicos informáticos que les provee la Entidad para el desempeño de sus funciones laborales y contractuales.

6.2.8. Procesos disciplinarios

Todos los incidentes de seguridad de la información presentados en la UApA deben tener el tratamiento adecuado y establecido en el procedimiento de atención de incidentes de seguridad de la información, con el fin de determinar sus causas y responsables.

Del resultado de los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad y teniendo en cuenta el impacto y las responsabilidades identificadas, se

tomarán acciones y se realizará el respectivo traslado ante las instancias correspondientes.

En lo pertinente a la violación de las políticas de seguridad de la información de la Entidad, a los colaboradores y terceros, se les aplicará lo establecido en la ley, particularmente en el Código Único Disciplinario (Ley 734 de 2002), el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las adicionen, modifiquen, reglamenten o complementen.

6.3. Uso del Correo Electrónico

Define las directrices generales del buen uso del correo electrónico en la UApA.

Usos aceptables del servicio

Se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desempeñar en la Unidad y no se debe utilizar para otros fines.

Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen de la UApA.

Todos los colaboradores y terceros que son autorizados para acceder a la red de datos y los componentes de tecnologías de Información son responsables de todas las actividades que se ejecuten con sus credenciales de acceso a los buzones de correo.

Todos los colaboradores y terceros deben dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la información de la Unidad.

El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa en relación con la Unidad. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad de la UApA y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.

Cuando un Proceso, Oficina, Grupo o Dependencia, tenga información de interés institucional para divulgar, lo debe hacer a través de la Oficina Asesora de Comunicaciones de la UApA, o el medio formal autorizado para realizar esta actividad.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la UApA y deberán conservar en todos los casos el mensaje legal corporativo.

El único servicio de correo electrónico controlado en la entidad es el asignado directamente por la Subdirección de Información de la Unidad, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.

El servicio de correo electrónico cuenta con respaldo de información (Back up) de diferentes procesos aplicados de manera periódica y segura.

Se realiza copia de respaldo de Información a los registros de auditoria que generan los buzones de correo.

Los demás servicios de correo electrónico son utilizados bajo responsabilidad directa y riesgo de los usuarios, siendo necesaria la aprobación y firma por parte del director, Asesor, Subdirector, Coordinador de Grupo de Trabajo o Supervisor de contrato; de un documento de análisis de riesgos para la autorización de sistemas de correo electrónico diferentes al institucional.

Para acceder al correo electrónico desde canales externos a los de la Unidad, se debe garantizar que la información viaja cifrada.

Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo a los niveles de clasificación para los cuales se requiere etiquetado (Reservado o Confidencial), de acuerdo a la Clasificación y Etiquetado de la Información establecida en la entidad.

El tamaño del buzón de correo electrónico se asigna de manera estandarizada, la capacidad específica es definida y administrada por la Subdirección de Información de la Unidad.

Todos los Colaboradores y Terceros son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro de la UApA, para que de esta forma la SDI realice el ajuste de permisos requerido.

El usuario debe reportar cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos de dudosa procedencia o con virus a la SDI, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos. De la misma forma el usuario debe reportar cuando no reciba correos y este seguro que este no es de tipo SPAM, así la SDI realizará el análisis respectivo para evaluar el origen y así tomar las medidas pertinentes.

Cuando un Colaborador se retire de la UApA y se le haya autorizado el uso de una cuenta con acceso a la red y al servicio de correo corporativo, debe notificar a la SDI la desactivación de la cuenta.

Los mensajes y la información contenida en los buzones de correo son de propiedad de la UApA.

Cada usuario se debe asegurar que, en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios correctos. Si tiene listas de distribución también se deben depurar. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

La información almacenada en los archivos de tipo .PST es responsabilidad de cada uno de los usuarios y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.

Las cuentas institucionales (Ejemplo: Comunicaciones, atención al ciudadano, comunicaciones judiciales, control interno etc.) deben tener una persona responsable que haga depuración del buzón periódicamente.

Todo colaborador es responsable de reportar los mensajes cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el colaborador o tercero desconfíe del remitente de un correo electrónico debe remitir la consulta a la mesa de ayuda de la SDI.

Si una cuenta de correo es interceptada por personas mal intencionadas o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), la SDI actuará según sea el caso.

La Subdirección de Información se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo. Si el virus u otro programa destructivo no pueden ser eliminados, el mensaje será borrado.

Ningún colaborador o tercero debe suscribirse en boletines en líneas, publicidad o que no tenga que ver con sus actividades laborales, con el correo institucional.

El funcionario, Colaborar o Tercero no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario, debe notificar a la SDI, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo de la UApA.

Las cuentas creadas en los dominios de Alimentos para Aprender serán bloqueadas automáticamente después de estar inactivas en un tiempo de noventa (90) días, para el desbloqueo de la cuenta se debe hacer a través de una mesa de ayuda de tecnología.

Todos los usuarios de correo electrónico, el tamaño máximo para recibir o enviar mensajes es de 25 MB (incluyendo la suma de todos los adjuntos).

Usos no aceptables del servicio

Envío de correos masivos que no hayan sido previamente autorizados a través del procedimiento formal de Solicitud de Cuentas de Usuario, establecido en la UApA.

Envío, reenvío o intercambio del mensajes no deseados o considerados como SPAM, cadena del mensajes o publicidad.

Envío o intercambio del mensaje con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

Envío o intercambio del mensaje que promuevan la discriminación sobre la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

Envió del mensaje que contengan amenazas o mensajes violentos.

Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.

Divulgación no autorizada de información propiedad de la UApA. Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.

Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

Adulterar o intentar adulterar mensajes de correo electrónico. Enviar correos masivos, con excepción de con nivel de director o superior, quienes sean previamente autorizados por estos para ello, o de que en calidad de sus funciones amerite la excepción.

Enviar correos masivos, con excepción de con nivel de director o superior, quienes sean previamente autorizados por estos para ello, o de que en calidad de sus funciones amerite la excepción.

Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado “Usos aceptable del servicio” del presente lineamiento.

6.4. MANEJO DE INTERNET

Definir los lineamientos y directrices del buen uso del internet, con el fin de asegurar una adecuada protección de la información de la UApA.

Usos aceptables del servicio

Este servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación en la UApA y no debe utilizarse para ningún otro fin.

Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la Entidad o que afecte la seguridad de la información.

Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.

El navegador autorizado para el uso de Internet en la red de la UApA es el instalado por la SDI, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para prevenir ataques de virus, spyware y otro tipo de software o código malicioso.

No se permite la conexión de módems externos o internos en la red de la Unidad, previa solicitud autorizada por SDI.

Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades dentro de la UApA.

Todos los usuarios son responsables del uso de sus credenciales de acceso a las cuales les fue otorgado el acceso a internet.

Para realizar intercambio de información de propiedad de la Unidad con otras entidades, se debe seguir un proceso formal de requisición de la información, el cual debe contar con la previa autorización del dueño de la información.

La UApA se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.

Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información y la seguridad de la información, entre otros.

Los colaboradores y tercero de la UApA no deben asumir en nombre de la entidad, posiciones personales en encuestas de opinión, foros u otros medios similares.

Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la Unidad.

Usos no aceptables del servicio

Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite.

Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.

Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de los presentes lineamientos.

Todos los usuarios invitados que requieran acceso a internet dentro de las instalaciones la UApA deben realizarlo por medio de la red WIFI invitados y cumplir con los requerimientos que el portal solicita, una vez que tengan acceso al servicio de internet, deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.

No se permite el acceso a páginas con contenido restringido como pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p) o páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración de contenidos de la UApA y las emitidas por los entes de control.

No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

6.5. USO DE REDES SOCIALES

Definir los lineamientos para el uso del servicio de Redes sociales por parte de los usuarios autorizados en la Unidad.

Usos aceptables del servicio

Todos los usuarios autorizados para hacer uso de los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la Unidad.

El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas la UApA.

Es permitido el uso de redes sociales utilizando video conferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información de la Entidad.

La UApA facilita el acceso a estas herramientas, teniendo en cuenta que constituyen un complemento de varias actividades que se realizan por estos medios y para el desempeño de las funciones y actividades a desempeñar por parte de los colaboradores y terceros, sin embargo es necesario hacer buen uso de forma correcta y moderada.

Usos no aceptables del servicio

No se deben descargar programas ejecutables o archivos que puedan contener software o código malicioso.

No se permiten descargas, distribución de material obsceno y no autorizado, degradante, terrorista, abusivo o calumniante a través del servicio de Redes Sociales.

No se debe practicar e intentar acceder de forma no autorizada a los sistemas de seguridad del servicio de Internet de la UApA, o aprovechar el acceso a Redes Sociales para fines ilegales.

Es claro que no se puede difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.

Todos los Colaboradores y erceros de la Unidad, deben seguir los procedimientos y planes de comunicaciones interna y externa.

La Subdirección de Información, será la encardo de determinar las directrices y lineamientos para el uso de las diferentes herramientas o plataformas de redes sociales en la UApA, previo acuerdo con la Oficina Asesora de Comunicaciones.

6.5 USO DE RECURSOS TECNOLÓGICOS

Alimentos para Aprender asigna los recursos tecnológicos necesarios como herramientas de trabajo para el desempeño de las funciones y actividades laborales de los colaboradores.

Cada equipo de cómputo está configurado con el Hardware y Software básico necesario para su funcionamiento:

- Sistema operativo: Windows, IOS o Linux
- Ofimática: Office 365 (Acces, Excel, OneNote, One Drive, Outlook, Power Point, Word.)
- Descomprimir Archivos: Winzip
- Antivirus
- Video conferencia - Chat: Teams

La instalación de software se encuentra bajo la responsabilidad la SDI y por tanto son los únicos autorizados para realizar esta actividad y toda solicitud debe realizarse a través de la Mesa de Ayuda de Tecnología.

Si los colaboradores cuentan en los equipos de cómputo con aplicaciones diferentes a las antes mencionadas o con software no autorizado, se procederá a realizar la desinstalación sin previa autorización.

Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios únicamente deben ser realizados por la Subdirección de Información.

La SDI es la responsable de definir la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas en la UApA para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación del cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

Sólo el personal autorizado por la SDI podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la UApA. Las conexiones establecidas para este fin utilizan los esquemas de seguridad establecidos por la entidad.

Los colaboradores y terceros de la Entidad son responsables de hacer buen uso de los recursos tecnológicos de la Unidad y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros colaboradores, legislación vigente y políticas y lineamientos de seguridad de la información establecidas por la UApA.

La información clasificada como personal almacenada en los equipos de cómputo, medios de almacenamiento o cuentas de correo institucionales, debe ser guardada en su totalidad en una carpeta especificada para tal fin, la cual debe ser nombrada como “PERSONAL”.

Todo activo de propiedad de la UApa asignado a un colaborador o tercero, debe ser entregado al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos removibles.

Cualquier requerimiento que tenga un usuario respecto a instalación, desinstalación, o actualización de sus aplicaciones, deberá solicitarse por medio de la Mesa de Ayuda Tecnológica, y estas entrarán a ser evaluadas por la SDI para su aprobación o denegación.

El software propiedad de la UApA, es para uso exclusivo de usuarios de planta y contratistas con vínculo directo la UApA. Proveedores y/o contratistas no pueden instalar o hacer uso de las licencias de la Unidad.

Si un equipo de cómputo requiere seguir algún procedimiento de formateo o reinstalación de aplicaciones, por problema de infección de virus, o por algún daño que haya sufrido, se debe realizar una solicitud a la Mesa de ayuda de Tecnología, la cual respaldará la información y documentos que se consideren de las funciones asignas a su cargo.

Cada usuario debe ser responsable de sacar el respaldo respectivo de la información que maneja en su equipo de cómputo. La SDI sólo es responsable de respaldar y salvaguardar la información que se encuentra en los discos compartidos a través de los servidores del centro de cómputo. En caso de que algún usuario requiera ayuda con sus respaldos, deberá solicitarlo por medio de la Mesa de ayuda de Tecnología, para que este le implemente el procedimiento más adecuado y su información pueda estar asegurada.

El usuario no deberá alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos.

El usuario no deberá abrir los equipos de cómputo, como tampoco sacar o cambiar componentes de estos.

En caso de que un equipo de cómputo presente un mal funcionamiento, el usuario responsable por el equipo de cómputo deberá reportarlo de inmediato a través de la Mesa de ayuda de Tecnología. La Mesa de ayuda de Tecnología hará una evaluación del equipo para determinar el tipo de daño y la reparación que se requiere.

De la evaluación que se realice del equipo de cómputo dañado, se determinará lo siguiente:

- Si el equipo de cómputo está en garantía y el daño puede ser procesado por garantía. En este caso lo enviará al proveedor donde fue adquirido el equipo para que este haga la reposición de la parte defectuosa y devuelva el equipo lo más pronto posible.
- Si el equipo de cómputo está fuera de garantía, se determinará si el equipo puede reparase internamenteen el diario o se requiere de una reparación en un servicio técnico autorizado.
- Si el daño es por falla eléctrica, se determinará la parte que debe ser reemplazada y y si la reparación puede ser realizada en el diario o debe enviarse a una empresa de servicio técnico. Adicionalmente se reportará el particular a la Sudirección corporativa para que tomen las medidas pertinentes respecto al punto eléctrico que causó el problema.
- La Mesa de ayuda de Tecnología también evaluará la causa del daño del equipo y si se determina que es por mal uso del mismo, se procederá con la reparación, pero se informará a la SDI para que el costo de la reparación del mismo sea descontado al usuario responsable del equipo de cómputo.

El uso de dispositivos como unidades de almacenamiento USB, CD`s o cualquier otro, es de exclusiva responsabilidad de los usuarios, los cuales deberán asegurarse de que estos no contengan ningún medio de contaminación de virus.

Los equipos de cómputo suministrados por la UApA se entregarán mediante un acta de entrega/recepción en la cual se detallará todos los equipos que se entregan, sus componentes y el software que se le ha instalado (en caso de que aplique). A partir de

ese momento él usuario será responsable de los equipos y accesorios que le han sido entregados, de su cuidado y su buen uso.

En caso de que un equipo tipo móvil (sea este laptop o accesorios) sea hurtado o extraviado, el usuario deberá proceder de inmediato a reportarlo a la SDI mediante la Mesa de ayuda de Tecnología. En el caso de robo deberá presentar también la denuncia respectiva.

Cuando un usuario se retira de la UApA o cambia de función o cargo dentro de la misma debe realizar la devolución de todos los equipos de tecnología que le han sido asignado en el transcurso en que ha desempeñado su cargo. La subdirección de Gestión Corporativa es responsable de comunicar este particular a laSDI. Esta devolución estará sustentada por un acta de entrega/recepción.

La devolución debe realizarse a través de la Mesa de ayuda de Tecnología, la cual se encargará de comprobar que los equipos de cómputo sean devueltos en óptimas condiciones. En caso de que algún equipo de cómputo no sea devuelto, o sea devuelto en mal estado, la UApA procederá a realizar el descuento correspondiente por la reposición de dicho equipo de cómputo, el cual será descontado de su sueldo (en el caso de cambio de cargo), o de su liquidación (en caso de salida de la Unidad).

Dispositivos móviles

Se considera “usuarios de dispositivos móviles” a quienes por las características de sus funciones asignadas dentro de la Unidad, utilizan habitualmente un portátil, Smartphone, tableta, etc. dentro y fuera de la organización.

Uso del Software legal y Derechos de Autor

Los usuarios solo podrán utilizar software legalmente adquirido y/o autorizado por la UApA. En caso de presentarse algún tipo de reclamación por software ilegal, esta recaerá sobre el usuario responsable en donde se encontrase instalado dicho software, debido a que está atentando contra los derechos de autor.

En presentaciones, documentos, informes y demás documentos que utilicen los usuarios para funciones de su cargo, debe mencionarse la fuente de donde se extrajo la información.

Los usuarios no pueden realizar copias de software que se encuentre instalado o sea desarrollado por la UApA, para su distribución.

Acceso Inalámbrico

El uso de la red inalámbrica será exclusivo para usuarios de planta y contratistas con vínculo directo con la Unidad, se habilitará el servicio previa solicitud, justificación y autorización a la Mesa de ayuda de Tecnología. Para accesos a dispositivos móviles, se realizará solo previa solicitud y justificación a la Mesa de ayuda de Tecnología.

Si alguna persona externa a la Unidad necesita acceso a la red inalámbrica de la UApA, deberá solicitarlo accediendo a la red “INVITADO” suministrando unos datos y enviado la solicitud para aprobación.

La información que se maneja dentro de la Unidad, es propiedad de esta y no puede ser divulgada; a no ser que esté autorizado su divulgación.

6.6. CLASIFICACIÓN DE LA INFORMACIÓN

La clasificación de la Información al interior de la Unidad tiene como proposito asegurar que la información de la UApA sea clasificada, con el fin de que sea tratada y protegida adecuadamente.

Esquema de Clasificación de la Información

Toda la información de la UApA debe ser identificada y clasificada de acuerdo a los niveles de clasificación definidos por la Entidad.

La Subdirección de Información, la ofician Asesora Jurídica y la Gestión Documental son los responsables de definir las directrices de clasificación de la información y las medidas de tratamiento y manejo de la información.

De acuerdo con la clasificación establecida por la entidad y el manejo y almacenamiento de la información, se debe tener en cuenta lo siguiente:

- Acceso a la información sólo de personal autorizado.
- Llevar un registro formal de acceso a la información.

- Conservar y mantener los medios de almacenamiento de información en un ambiente seguro.

Etiquetado y manejo de Información

Todos los colaboradores y terceros cuando sea el caso, deben mantener organizado los archivos de gestión, siguiendo los lineamientos establecidos por el Proceso de Gestión Documental.

Los directores, Sudirectores, Coordinadores de Grupo deben establecer mecanismos de control de documentos, con el fin de garantizar y mantener la disponibilidad, integridad y confidencialidad de la información.

Todos los colaboradores y terceros, son responsables de la organización, conservación, uso y manejo de los documentos en los medios que son dispuestos por la Entidad.

Para una óptima administración de la información, la Subdirección de Información suministra tres (3) recursos de almacenamiento los cuales son: onedrive, sharepoint y fileserver.

Todas las dependencias de la UApA deberán enviar a un archivo central la documentación de forma ordenada y organizada, de acuerdo con los tiempos de retención establecidos en las Tabla de Retención Documental.

El Archivo Central de la UApA recibirá las transferencias documentales de acuerdo con cronograma anual de transferencia Documentales.

La plataforma tecnológica usada para salvaguardar, conservar y facilitar la información de los documentos en medios magnéticos debe garantizar los principios fundamentales de la seguridad como son la integridad, confidencialidad y disponibilidad de la información y por gestión documental usabilidad y acceso.

Se deberá definir procedimientos de etiquetado de la información, de acuerdo con el esquema de clasificación definido por la Unidad.

El etiquetado de información debe incluir la información física y electrónica. Las etiquetas de la información se deben identificar y reconocer fácilmente.

Se debe garantizar la conservación, uso y recuperación de la información contenida en medios digitales, físicos y otros.

Usos no aceptables

Hacer caso omiso, retardar o no entregar de manera oportuna las respuestas a las peticiones, quejas, reclamos, solicitudes y denuncias, de igual forma retenerlas o enviarlas a un destinatario que no corresponde o que no esté autorizado, que lleguen por los diferentes medios, presencial, verbal, escrito, telefónico, correo y web.

Dañar o dar como perdido los expedientes, documentos o archivos que se encuentren bajo su administración por la naturaleza de su cargo.

Divulgación no autorizada de los expedientes, documentos, información o archivos.

Realizar actividades tales como borrar, modificar, alterar o eliminar información de la UApA de manera malintencionada.

6.7. GESTIÓN DE ALMACENAMIENTO

La gestión de Almacenamiento hace referncia a la protección de la información de la UApA velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento.

Se restringe el uso de carpetas compartidas desde equipos de escritorio. Si el colaborador no adopta esta política la SDI no se hace responsable de la pérdida o infiltración de la información.

Las carpetas compartidas sobre la infraestructura ofrecida por SDI como File server, SharePoint, OneDrive, serán administradas por las áreas quienes velarán por el buen uso de la información y de las carpetas.

Se debe documentar los permisos y accesos sobre la carpeta compartida, usando los siguientes criterios:

- Permisos de Lectura
- Permisos de Escritura y modificación
- Permisos de Control Total.

Lo cuales serán documentados por la SDI a través de la Mesa de Ayuda de tecnología.

La información CLASIFICADA o RESERVADA, debe utilizarse en las carpetas destinadas en el file server, para que sean incluidos en las Políticas de respaldo de información a cinta (backup).

La información pública de las áreas de la institución debe utilizarse las carpetas destinadas en el OneDrive.

La información pública para uso interno de la institución debe utilizarse en las carpetas destinadas en el share point, para que sean incluidos en las Políticas de respaldo de información.

El administrador de cada carpeta deberá fijar el límite de tiempo durante el cual estará publicada la información y compartido el recurso en la infraestructura ofrecida por la SDI.

Cada área tendrá un único administrador que será autorizado con permisos de lectura y escritura quien administrará las carpetas y será responsable a que usuarios otorgará permisos sobre esta.

Los permisos de administrador serán gestionados por la SDI, a través de la mesa de ayuda de tecnología.

Cada administrador de las carpetas compartidas deberá realizar semestralmente una depuración de la información y notificar a la SDI los cambios realizados.

Las carpetas compartidas tendrán una cuota de 20 Gigas en Share point, si el área requiere mayor capacidad de almacenamiento debe justificarlo a la SDI para ajustar la cuota como se defina según acuerdo por las dos áreas.

Se prohíbe el acceso a las carpetas compartidas a colaboradores desde equipos de cómputo que no cuenten con antivirus corporativo actualizado.

Se prohíbe el acceso a carpetas compartidas a usuarios que no tengan una vinculación directa con la Unidad.

Se prohíbe la publicación de archivo ejecutables (.exe, bat y dll entre otros) en las carpetas compartidas de Onedrive, SharePoint, File server, si el área requiere usar

alguna de las extensiones mencionadas, debe justificarlo a la SDI para ajustar los lineamientosde común acuerdo en tre las áreas.

La SDI realizara monitoreo y revisiones periódicas, con el fin de velar por una correcta administración de las carpetas compartidas cada semestre.

Se prohíbe el uso carpetas para el almacenamiento de archivos personales, música, videos, imágenes y cualquier otro tipo de archivo no relacionados con el cumplimiento de la función del colaborador.

Los permisos a las carpetas compartidas administrados por la SDI sobre los diferentes ambientes (Pruebas, Certificaciones y Producción) se autorizarán a través de una mesa de ayuda de tecnología.

La SDI define que los nombres a los archivos y carpetas sean lo suficientemente significativo sin que sea demasiado extenso, y que no contengan nombres de los usuarios. Se establece como longitud máxima para un nombre de archivo, 256 caracteres (un carácter puede ser una letra, número o un símbolo).

El único medio de respaldo de la información para los colaboradores es OneDrive, el cual será configurado por la SDI.

Gestión y Disposición de medios removibles

Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD’s, DVD’s, dispositivos personales “USB”, discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la Unidad y su uso hasta finalización de su contrato o cese de actividades.

Toda la información clasificada como CONFIDENCIAL o RESERVADA que sea almacenada los clientes activos de información que se requiera de protección especial de acuerdo a la calificación otorgada en el levantamiento de activos de información, debe cumplir con las directrices de seguridad estipuladas para la protección de los mismo.

Se debe llevar el registro de todos los medios removibles De la UApA y mantenerlo actualizado.

Todos los medios removibles deben ser almacenados de manera segura.

La Subdirección de Información puede restringir que medios de almacenamiento removibles se conecten a los equipos de cómputo que sean propiedad de la Unidad o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción, con el fin de evitar fuga de información a través de medios removibles.

Los medios de almacenamiento removibles que se conecten a la red de datos de la UApA o que se encuentren bajo su custodia, están sujetos a monitoreo por parte de la SDI.

Todos los retiros de medios de almacenamiento de las instalaciones de la UApA, como discos duros externos, se deben realizar con la autorización del propietario del proceso misional, estratégico, mejora continua o de apoyo, a través del formato orden de salida de elementos.

Todos los medios de almacenamiento removibles propiedad de la UApA, deben estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante.

Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, Cintas, etc, con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

Borrado seguro

Todos los medios de almacenamiento que sean de propiedad de terceros y que sean autorizados por la UApA para su uso dentro de la red corporativa, deben contar con su respectivo soporte.

Todos los medios de almacenamiento que contengan información de la Unidad y que salgan de la Entidad y que no se les vaya a dar más uso, o que se vayan a dar de baja, deben seguir el procedimiento de borrado seguro definido por la UApA, el cual garantiza que la información no es recuperable (Aplica para medios de almacenamiento de equipos alquilados, equipos para pruebas de concepto, equipos de proveedores, discos duros externos, medios de almacenamiento externos o equipos que sean reasignados, formateados, reinstaladoso que por desgaste o falla sean retiradoso dados de baja).

Eliminar de forma segura (destrucción o borrado) los medios de almacenamiento que no se utilicen y que contengan información de la Unidad.

Trasferencia de medios físicos

Toda la información clasificada como CONFIDENCIAL o RESERVADA que se desee almacenar en medios removibles y que sean transportados fuera de las instalaciones de la Unidad, debe cumplir con las disposiciones de seguridad indicadas por la Subdirección de Información, específicamente aquellas referentes al empleo de técnicas de cifrado.

El transporte de los medios físicos se debe hacer mediante un medio de transporte confiable y seguro, tomando las medidas y precauciones necesarias para garantizar que los medios de almacenamiento sean transportados adecuadamente, de esta forma se evitar una afectación a la integridad y disponibilidad.

Se debe llevar un registro o cadena de custodia de los medios de almacenamiento físico que son transportados.

6.8. CONTROL DE ACCESO

Se definen las directrices generales para un acceso controlado a la información de la Unidad Administrativa Especial de Alimentación Escolar.

Control de Acceso a Redes y Servicios en Red

La UApA suministra a los usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales.

Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

Toda actividad que requiera acceder a los servidores, equipos o a las redes de la UApA, deberá contar con la debida autorización de la SDI.

La conexión remota a la red de área local de la UApA debe ser establecida a través de una conexión VPN segura aprovisionada por la entidad, la cual debe ser autorizada por SDI y que cuenta con el monitoreo y registro de las actividades necesarias.

La autenticación de usuarios remotos deberá ser aprobada por el jefe inmediato del usuario y bajo una solicitud con su respectivo formato a la mesa de ayuda de tecnología.

Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica, se efectúa el seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.

Gestión de Acceso a Usuarios

Se establece el uso de contraseñas individuales para determinar las responsabilidades de su administración.

Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire.

Las contraseñas deben contener Mayúsculas, Minúsculas, números y por lo menos un carácter especial y de una longitud mayor a 8 caracteres.

El sistema debe obligar al usuario a cambiar la contraseña por lo mínimo 1 vez cada 90 días.

Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por la mesa de de ayuda.

Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.

LA Subdirección de Información debe garantizar que las contraseñas se almacenen de forma cifrada utilizando un algoritmo de cifrado unidireccional.

Cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware (por ejemplo apliance, impresoras, routers, switch, herramientas de seguridad, etc.).

No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, Jefes u otras personas que lo soliciten.

Todos los usuarios deben dar cumplimiento a las políticas de seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

Reportar a la SDI sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.

Las contraseñas de acceso a los servidores y administración de los Sistemas de Información deben ser cambiadas mínimo cada seis (6) meses.

El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de la Plataforma y Sistemas de Información debe estar autorizado por la SDI.

Todo equipo de cómputo que requiera acceso a la red interna de la UApA deberá tener como mínimo las siguientes medidas de seguridad: solución de anti-malware instalada y actualizada, parches de seguridad al día y mecanismos de autenticación habilitado para el ingreso a la red.

Revisión de los derechos de acceso de los Usuarios

Los derechos de acceso de los usuarios a la información y a la Plataforma Tecnológica y de procesamiento de información de la UApA debe ser revisada periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.

Retiro de los derechos de acceso

Cada uno de los procesos de la Entidad es responsable de comunicar a la Subdirección de Gestión Coorporativa, el cambio de cargo, funciones o actividades o la terminación contractual de los colaboradores pertenecientes al proceso. La Subdirección de Gestión Coorporativa es la encargada de comunicar a la Subdirección de Información sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

6.9. SEGURIDAD FÍSICA Y DEL ENTORNO

Los lineamientos en cuanto a Seguridad Física y del Entorno proponen evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información de la UApA.

Perímetro de Seguridad Física

Todas las entradas que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todos los Colaboradores y Terceros autorizados evitar que las puertas se dejen abiertas.

Todos los visitantes, sin excepción, deben portar la tarjeta de identificación de visitante o escarapela en un lugar visible mientras permanezcan en un lugar dentro de las instalaciones de la Unidad.

Todos los Colaboradores, Terceros y visitantes cuando sea el caso, sin excepción deben portar su carnet o escarapela en un lugar visible mientras permanezcan dentro de las instalaciones de la Unidad.

Los visitantes deben permanecer acompañados de un colaborador de la Unidad, cuando se encuentren en las oficinas o áreas donde se maneje información.

Es responsabilidad de todos los colaboradores y terceros de la UApA borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se debe dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.

Los visitantes que requieran permanecer en las instalaciones de la UApA por periodos superiores a dos (2) días deben ser presentados al personal de oficina donde permanecerán.

El horario autorizado para recibir visitantes en las instalaciones de la Unidad es de 8:00 AM a 5:00 PM. En horarios distintos se requerirá de la autorización de los directores, subdirectores o Coordinador de Grupo correspondientes.

Los dispositivos removibles, así como toda información CONFIDENCIAL de la UApA independientemente del medio en que se encuentre, deben permanecer bajo seguridad durante horario no hábil o en horarios en los cuales el colaboradores o terceros responsable no se encuentre en su sitio de trabajo.

Las instalaciones de la UApA deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de colaboradores y terceros y visitantes.

Controles de Acceso Físico

Las áreas seguras dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

En las áreas seguras, en ninguna circunstancia se puede fumar, comer o beber.

Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un o colaborador del proceso. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

Se debe contar con al menos dispositivos de control de acceso físico a los Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, el cual garantice el acceso a solo el personal autorizado.

Ubicación y Protección de los equipos.

La plataforma tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

Seguridad de los equipos fuera de las instalaciones

Los equipos portátiles que contengan información clasificada como CONFIDENCIAL o RESERVADA, deben contar con controles de seguridad que garanticen la confidencialidad de la información.

Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En casos de viaje siempre se debe llevar como equipaje de mano.

En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente a la Subdirección de Gestión Coorporativa y la SDI y debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de la misma.

Cuando los equipos portátiles se encuentren desatendidos deben estar asegurados con una guaya, dentro o fuera de las instalaciones de la UApA.

Para el caso de los equipos que cuentan con puertos de transmisión y recepción de infrarrojo y Bluetooth estos deben estar deshabilitados.

Todos los equipos de cómputo deben ser registrados al ingreso y al retirarse de las instalaciones de la UApA.

Seguridad en la reutilización o eliminación de los equipos

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

Retiro de Activos

Ningún equipo de cómputo, información o software debe ser retirado de la UapA sin una autorización formal. Se debe realizar periódicamente comprobaciones puntuales para detectar el retiro no autorizado de activos de la Unidad.

6.10. ESCRITORIO Y PANTALLA DESPEJADA

Se presentan los lineamientos generales para mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información de la Unidad.

Todo el personal de la UApA debe conservar su escritorio libre de información propia de la entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

Todo el personal de la UApA debe bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de ellos o que por cualquier motivo deban dejar su puesto de trabajo.

Todos los usuarios al finalizar sus actividades diarias deben salir de todas las aplicaciones y apagar las estaciones de trabajo.

Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deben reutilizar papel que contenga información CONFIDENCIAL.

En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios deben dejar la información CONFIDENCIAL protegida bajo llave.

6.11. GESTIÓN DE CAMBIOS

La Gestión de Cambios asegurará que los cambios a nivel de infraestructura, aplicaciones y sistemas de información realizados en la Unidad se realicen de forma controlada.

Se deben establecer procedimientos para el control de cambios ejecutados en la entidad.

Toda solicitud de cambio en los servicios de infraestructura y sistemas de información de la UApA, se debe realizar siguiendo los procedimientos de Gestión de Cambios, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información.

Se debe llevar una trazabilidad del control de cambios solicitados.

En el procedimiento de gestión de cambios se debe especificar los canales autorizados para la recepción de solicitudes de cambios, correo electrónico o un oficio dirigido al Subdirector de Información.

Se debe establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware.

Se deben especificar en qué momento existen cambios de emergencia en la cual se debe garantizar que los cambios se apliquen de forma rápida y controlada.

Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los colaboradores o terceros que por sus funciones tienen relación con el sistema de información.

Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.

Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente.

Se debe disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.

6.12. PROTECCIÓN CONTRA CÓDIGO MALICIOSO

Los siguientes lineamientos definen las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en la Unidad.

Toda la infraestructura de procesamiento de información de la UApA, cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores de la UApA.

Se debe restringir la ejecución de código móvil, aplicando políticas a nivel de sistemas operativos, navegadores y servicio de control de navegación.

Todos los colaboradores y terceros que hacen uso de los servicios de tecnología de la información y comunicaciones de la Unidad son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

Alimentos para Aprender cuenta con el software necesario como antivirus para protección a nivel de red y de estaciones de trabajo, contra virus y código malicioso, el servicio es administrado por la Subdirección de Información.

El antivirus adquirido por la Unidad, sólo debe ser instalado por los responsables de la Subdirección de Información.

Los equipos de terceros que son autorizados para conectarse a la red de datos de la UApA deben tener antivirus y contar con las medidas de seguridad apropiadas.

Todos los equipos conectados la red de la UApA pueden ser monitoreados y supervisados por la SDI.

Se debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.

Se debe hacer revisiones y análisis periódicos del uso de software no malicioso en las estaciones de trabajo y servidores. La actividad debe ser programada de forma automática con una periodicidad semanal y su correcta ejecución y revisión estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones.

La Entidad debe contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.

Se deben hacer campañas de sensibilización a todos los colaboradores y terceros de ser de la UApA, con el fin de generar una cultura de seguridad de la información.

Los colaboradores de la UApA pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los colaboradoresy terceros cuando sea necesario siempre podrán consultar a la SDI sobre el tratamiento que debe darse en caso de sospecha de malware.

Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.

Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por MEN, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta establecida para ello.

El único servicio de antivirus autorizado en la entidad es el asignado directamente por la SDI, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura. Excepcionalmente se podrá realizar la ejecución de otro programa antivirus, únicamente por personal autorizado por la SDI para efectos de reforzar el control de presencia o programación de virus o código malicioso.

La Subdirección de Información es la responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los equipos de cómputo conectados a la red de la Unidad.

La Subdirección de Información se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.

La SDI se reserva el derecho de filtrar los contenidos que se trasmitan en la red de la Unidad, con el fin de evitar amenazas de virus.

Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.

6.13. BACKUP

Los lineamientos y directrices del Backup proporcionarán medios de respaldo de información adecuados en la UApA para asegurar la información crítica y que el software asociado se pueda recuperar después de una falla.

La Subdirección de Información debe realizar periódicamente un análisis de las necesidades del negocio para determinar la información crítica que debe ser respaldada y la frecuencia con que se debe realizar.

La Subdirección de Información junto a los subdirectores de las diferentes dpendencias de la Unidad deben determinar los requerimientos para respaldar la información y los datos en función de su criticidad, para lo cual se debe elaborar y mantener el inventario de activos de TI.

La Oficina de Tecnología y Sistemas de Información debe disponer y controlar la ejecución de las copias, así como la prueba periódica de su restauración. Para esto se debe contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información y del software crítico de la Unidad. Se debe definir y documentar un esquema de respaldo de la información.

El dueño de la información es responsable de definir claramente el periodo de retención de respaldos, en función de los requerimientos de las áreas funcionales.

Se debe tener en cuenta los lineamientos de la ley 594 de 2000 o cualquiera que la modifique, adicione o derogue.

Se debe verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de garantizar la integridad y disponibilidad de la información.

Se deben definir procedimientos para el respaldo de la información, que incluyan los siguientes parámetros:

- Establecer un esquema de rotulado de las copias de respaldo, que contengan toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.

- Definir un el procedimiento de reemplazo de los medios de almacenamiento de copias de respaldo, una vez terminada la posibilidad de ser reutilizados de acuerdo a lo indicado por el proveedor, y asegurar la destrucción de los medios de información retirados o desechados.
- Almacenar en una ubicación remota o externa las copias de respaldo recientes de información, junto con registros completos de las mismas y sus procedimientos documentados de restauración.
- Se deben retener por lo menos por tres periodos los activos de información de la Unidad.
- Para realizar las copias de respaldo en el sitio remoto, se debe tener en cuenta el nivel de clasificación otorgado por la Entidad a los que se encuentre sujeta.
- Se deben asignar los niveles de protección física y ambiental adecuada a la información de respaldo según las normas aplicadas y las especificaciones dadas por el fabricante.
- Se deben extender los mismos controles de seguridad aplicados a los activos de TI en el sitio principal al sitio alterno.

La Subdirección de Información, a través del Administrador de Bases de Datos, de la Red y servidores, debe:

- Actualizar periódicamente las configuraciones de los Servidores para la correcta ejecución de las copias de respaldo.
- Efectuar las copias de información de los Servidores, cada vez que se realice un cambio significativo en los Sistemas Operativos o configuraciones Básicas.
- Realizar un respaldo Diferencial semanalmente de los Servidores de Base de Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.
- Realizar un respaldo full mensual de los Servidores de Base de Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.
- Realizar un respaldo full anual de los Servidores de Base de Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.
- Las copias de respaldo se deben realizar en horario no hábil.
- Los dispositivos magnéticos que contienen información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra almacenada.
- El sitio alterno donde se almacenan las copias de respaldo debe contar con los controles de seguridad necesarios, para cumplir con las medidas de protección y seguridad física apropiados.

- Conservar los medios de almacenamiento de información en un ambiente que cuente con las especificaciones emitidas por los fabricantes o proveedores.

Registro de Respaldo de Información

LA UApA contará con un servicio de Respaldo de la Información (NAS), donde se iran cargando los Backups con replicación. Dichos procedimientos estaran a cargo del Administrador de Bases de Datos, Redes y Servidores.

La información respaldada debe ser probada como mínimo dos veces al año, asegurando que es confiable, integra y que se estará disponible en el evento que se requiera para su utilización en casos de emergencia.

Se deben probar los procedimientos de restauración, para asegurar que son efectivos y que pueden ser ejecutados en los tiempos establecidos.

Se debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información.

La Subdirección de Información, a través del Administrador de la Base de Datos, de Red y Servidores, debe aplicar los siguientes lineamientos:

- Restaurar por lo menos cada seis meses, el escenario adecuado para probar las copias de respaldo de los Servidores.
- Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.
- Validar la integridad y accesibilidad de las cintas magnéticas por lo menos cada cuatro meses.
- Mantener siempre una copia de la información de los Servidores, por lo menos con una antigüedad no superior a 24 horas.
- Se debe mantener un monitoreo frecuente sobre el rendimiento y alcance de la información en la Base de Datos para así asegurar la integridad de la información respaldada.

Respaldo de Información para Usuarios Finales

Todos los usuarios son responsables de realizar los respaldos de información personal almacenada en los equipos asignados.

Toda la información relevante a las funciones del colaborador debe ser almacenada en el Onedrive suministrado por la SDI.

La Subdirección de Información, debe mantener los respaldos de información en condiciones adecuadas de medio ambiente, temperatura, humedad, y otros.

Ningún usuario puede realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto puede ser denominado fuga de información.

Todos los colaboradores y terceros de la UApA deben dar estricto cumplimiento a estos Lineamientos y el que haga caso omiso puede ser sujeto a acciones disciplinarias o civiles, incluyendo la terminación del respectivo contrato.

Se debe elaborar un plan de emergencia para todas las aplicaciones que manejen información crítica de la Entidad, el responsable de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.

Es responsabilidad todos los colaboradores y terceros almacenar la información crítica asociada con su labor en el servidor de archivos establecido, para garantizar que la información está siendo respaldada.

6.14. GESTIÓN DE SEGURIDAD DE LAS REDES

Los lineamientos en cuanto a la Gestión de Seguridad de las Redes establecen los controles necesarios para proteger la información de Alimentos para Aprender desde la Red interna.

La Subdirección de Información es la responsable de administrar y gestionar la red de la UApA. Así mismo es la responsable de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

La UApA proporciona a los colaboradores y terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por la SDI.

El trabajo a través de medios remotos a la red de la UApA, se permitirá de acuerdo a la Política y lineamientos de Teletrabajo establecida por la Entidad.

Separación de las Redes

La UApA debe establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.

Se deben seguir los procedimientos de acceso o retiro de componentes tecnológicos para la solicitud de servicios de red.

Se deben establecer parámetros técnicos para la conexión segura de la red con los servicios de red.

Se deben establecer mecanismos de autenticación seguros para el acceso a la red.

Se deben separar las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.

6.15 SEGURIDAD DE LA INFORMACIÓN - RELACIONES CON PROVEEDORES

Los lienamientos de seguridad de la Información – Relaciones con Proveedores establecen los criterios de seguridad la información para la información accedida por proveedores.

Consideraciones de seguridad en los acuerdos con terceras partes

En todos los Contratos o Acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Entidad, se deben realizar Acuerdos de Confidencialidad sobre el manejo de la información.

Los Acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio.

Dentro del contrato o acuerdo se deben definir claramente el tipo de información que se va a intercambiar por las partes.

6.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los lineamientos hacia la Gestión de incidentes de seguridad estan encaminados a gestionar todos los incidentes de seguridad reportados en la UApA, adecuadamente, dando cumplimiento a los procedimientos establecidos.

Reporte sobre los eventos y las debilidades de la seguridad de la información
Todos los colaboradores y terceros de la entidad tienen la responsabilidad de reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.

Se debe dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados. Así como tambien establecer las responsabilidades en la Gestión de Incidentes de Seguridad de la Información.

Se debe definir el procedimiento de atención de incidentes de seguridad de la información de la UApA.

Se debe llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos.

Se debe recolectar las evidencias (CCP, Fiscalía, colcert, mintic) necesarias lo más pronto posible después del reporte del incidente.

Escalar los incidentes a niveles superiores en caso de que sea requerido.

Se debe hacer evaluaciones de los incidentes presentados ya que se puede necesitar de controles adicionales.

Se debe realizar sensibilización a todos los usuarios sobre incidentes de seguridad de la información.

7. BIBLIOGRAFIA

- Política de Seguridad y Privacidad de la Información MEN

- Departamento Administrativo de la Función Pública, Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano.
- Guías del modelo de seguridad y privacidad emitidas por MINTIC. Departamento Administrativo de la Función Pública, Guía para la administración del riesgo.
- Departamento Administrativo de la Función Pública, Planeación de los Recursos Humanos- Lineamientos de política, estrategias y orientaciones para la implementación.
- Presidencia de la República - Secretaría de Transparencia, Documento “Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.
- Presidencia de la Republica – Alta Consejería Presidencial para el Buen Gobierno y la Eficiencia Administrativa, Modelo Integrado de Planeación y Gestión.
- Norma técnica ISO 27001:2013 Norma técnica ISO 27005:2013

HISTORIAL DE CAMBIOS

VERSIÓN	OBSERVACIONES	FECHA
1	Se crea el documento	Febrero de 2021