Unidad de Planeación de Infraestructura de Transporte

Políticas Técnicas de Seguridad de la Información

1. Política

Las Políticas Técnicas de Seguridad de la Información son el conjunto de declaraciones y decisiones formalmente adoptadas por la UPIT para la protección de la confidencialidad, integridad y disponibilidad de la información institucional.

Estas políticas contemplan los controles que deben cumplir todos los funcionarios y contratistas de la UPIT y las partes interesadas en los servicios e información que genera la Entidad y atiende los lineamientos de seguridad recomendados por el modelo de seguridad y privacidad de la información de MINTIC y la norma técnica colombiana NTC ISO/IEC 27001 en su versión vigente.

2. Objetivo

Brindar la orientación necesaria a todos los colaboradores de la UPIT y las partes interesadas, sobre los controles de seguridad que se deben implementar y cumplir para reducir las posibilidades de eventos de seguridad de la información no deseados que puedan afectar el cumplimiento de la misión y objetivos de la Unidad de Planeación de Infraestructura de Transporte.

3. Alcance

Las Políticas Técnicas de Seguridad de la Información cubren los controles en aspectos organizacionales, de seguridad del talento humano y controles de seguridad física tecnológicos que todos los procesos y colaboradores de la UPIT deben aplicar para preservar la seguridad de la información institucional.

4. Políticas técnicas de seguridad de la información

4.1. Organización general de la seguridad de la información

4.1.1. Política general de la seguridad de la información

La Unidad de Planeación de Infraestructura de Transporte gestiona los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de toda la

información necesaria para planear el desarrollo sostenible de la infraestructura de transporte del país, a través de su Sistema de Gestión de Seguridad de la Información, el cual mejorará continuamente con:

1. La implementación de las acciones que permitan cumplir los requisitos legales y normativos en materia de seguridad de la información que sean aplicables a su misionalidad.
2. La adopción de los controles de seguridad de la información que faciliten y aseguren las actividades de sus diferentes procesos institucionales.
3. El entrenamiento de todos sus colaboradores en materia de seguridad de la información.
4. La Identificación, valoración y tratamiento de los riesgos de seguridad de la información que puedan afectar a todos sus procesos institucionales.

Como objetivos de su sistema de gestión de seguridad de la información, la UPIT se compromete a:

1. Mantener todos los riesgos que puedan afectar la seguridad de la información dentro de los limites tolerables definidos en el manual de administración y gestión de riesgos.
2. Sensibilizar a todos los colaboradores de la UPIT y a las partes interesadas pertinentes en los aspectos relevantes en materia de seguridad de la información necesarios para impedir la materialización de incidentes de seguridad de la información que afecten a la Entidad.
3. Fomentar la adopción de la cultura de autogestión en la protección de la información institucional en todos los colabores de la UPIT a través de acciones que mejoren el cumplimiento de las políticas, procedimientos y controles de seguridad y privacidad de la información.
4. Mantener y mejorar la infraestructura tecnológica y los controles necesarios para garantizar la disponibilidad, confidencialidad e integridad de la información institucional.

4.1.2. Roles y responsabilidades en materia de seguridad de la información

La Unidad de Planeación de Infraestructura de Transporte – UPIT asigna las funciones relacionadas con la seguridad de la información de acuerdo con los procedimientos institucionales que definen los manuales de funciones para los diferentes cargos de la Entidad. Los contratistas y proveedores de servicios cumplen con las obligaciones en materia de seguridad de la información y se comprometen a seguir las políticas de seguridad de la información como lo establecen las cláusulas de sus respectivos contratos.

El seguimiento y control al desempeño de las acciones de implementación de la Política de Seguridad Digital del Modelo Integrado de Planeación y Gestión es liderado por el Comité Institucional de Gestión y Desempeño.

4.1.3. Segregación de deberes

Los roles y responsabilidades de acuerdo con la gestión de la seguridad se controlan mediante segregación de funciones que permiten establecer: a) roles con responsabilidades de autorización de acciones y; b) roles con responsabilidad de ejecución de actividades, lo que permite la implementación adecuada del Sistema Integrado de Gestión y Control, garantiza la trazabilidad de las acciones realizadas sobre el tratamiento y gestión de los activos de información y facilita la implementación de un ambiente de control que reduce riesgos asociados al abuso de privilegios.

La descripción de la segregación de deberes se documenta en los diferentes documentos institucionales, como el Manual Específico de Funciones y Competencias Laborales que establece las responsabilidades de los servidores de la UPIT y los contratos de prestación de servicios en donde se definen las responsabilidades de los colaboradores de la Entidad en materia de seguridad de la información.

4.1.4. Responsabilidades de la Alta Dirección

La máxima autoridad en la adopción de políticas de seguridad y privacidad de la información es el Comité Institucional de Gestión y Desempeño.

El Comité demuestra su compromiso con la implementación de la seguridad de la información en la UPIT mediante:

- Divulgación del Sistema de Gestión de Seguridad de la Información y sus objetivos.
- Divulgación de la Política de Gestión de la Seguridad de la Información y Protección de Datos Personales.
- Aplicación de la Política de Gestión de Riesgos Institucionales que considera el tratamiento de los riesgos de seguridad de la información y protección de datos personales.
- Revisión de las propuestas de los recursos necesarios para mantener y mejorar el Sistema de Gestión de Seguridad de la Información.
- Revisión del estado de riesgos residuales en materia de seguridad de la información y protección de datos personales.

- Revisión de las acciones que aseguren que el Sistema de Gestión de Seguridad de la Información es conveniente y adecuado a las necesidades de protección de los activos de información de la UPIT.
- Seguimiento a las acciones de mejora del Sistema de Gestión de Seguridad de la Información.

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es el responsable de liderar la gestión de la seguridad de la información en la Entidad y demuestra su compromiso con la gestión de la seguridad de la información mediante:

- Liderazgo en el diseño estratégico del Sistema de Gestión de Seguridad de la Información y Protección de Datos Personales.
- Gestión de la totalidad del ciclo de vida del Sistema de Gestión de Seguridad de la Información, desde su planificación hasta su revisión y mejora, aplicando el ciclo Planear, Hacer, Verificar y Actuar.
- Liderazgo en el ciclo de gestión del riesgo de seguridad de la información mediante dirección y orientación a las dependencias de la UPIT en las acciones de: identificación, valoración, selección de estrategias de gestión de riesgo y la implementación y mantenimiento de los controles de seguridad.
- Elaboración y presentación de los reportes de avance de la implementación del Sistema de Gestión de Seguridad de la Información.
- Elaboración del Plan de Gestión de Seguridad de la Información y su articulación con el Plan de Acción Anual Institucional.
- Coordinación de la aplicación de los procedimientos y controles necesarios para garantizar la seguridad de la información en los términos definidos por el Comité Institucional de Gestión y Desempeño.
- Mantenimiento y actualización de las Políticas de Seguridad de la Información y los procedimientos necesarios para el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información de acuerdo con los cambios identificados en el entorno y los requerimientos de las partes interesadas.
- Elaboración e implementación de reportes, internos y externos requeridos por las partes interesadas para evidenciar el cumplimiento de las obligaciones legales en materia de seguridad de la información.
- Evaluación de la efectividad de las medidas de control ejecutadas para el tratamiento de los riesgos de seguridad de la información identificados
- Monitorización del perfil de riesgo de seguridad de la información y socialización de su evaluación al Comité Institucional de Gestión y Desempeño.
- Seguimiento permanente a los procedimientos y planes de acción relacionados con la gestión de riesgos de seguridad de la información.
- Seguimiento a las medidas adoptadas para mitigar el riesgo inherente de seguridad de la información con el propósito de evaluar su efectividad.

- Elaboración de propuestas de campañas de sensibilización en seguridad de la información.
- Coordinación, evaluación e implementación de las acciones de mejora sobre el Sistema de Gestión de Seguridad de la Información.
- Apoyo a las actividades necesarias para realizar la revisión y evaluación interna y externa del estado del Sistema de Gestión de Seguridad de la Información.

4.1.5. Contacto con las autoridades

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de autorizar contacto con las autoridades y grupos especializados en materia de seguridad de la información entre otros:

- Ante la Superintendencia de Industria y Comercio cuando el incidente tiene relación con protección de datos personales.
- Ante la Fiscalía General de la Nación cuando el incidente de seguridad de la información constituye delito informático.
- Ante el centro de respuesta de incidentes la Policía Nacional (CSIRT PONAL) cuando se requiera apoyo en el tratamiento de evidencias forenses de delitos informáticos.
- Ante el Centro de Respuesta ante incidentes de seguridad de la información de la COLCERT cuando se evidencien ataques informáticos o se requiera apoyo técnico especializado en materia de seguridad de la información.

4.1.6. Contacto con grupos de intereses en seguridad de la información

Cuando sea conveniente, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones podrá autorizar el intercambio de información sobre amenazas informáticas con los grupos de interés en materia de seguridad de la información, ciberseguridad y protección de datos personales.

En ese sentido, podrá establecer relacionamiento en materia de seguridad de la información, ciberseguridad y protección de datos personales con grupos de interés como organizaciones gubernamentales nacionales o internacionales, grupos de investigación reconocidos en el sector de la seguridad de la información o proveedores de servicio.

Los contactos autorizados serán gestionados por el Coordinador del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones a través del profesional responsable del Sistema de Gestión de Seguridad de la Información.

4.1.7. Inteligencia de amenazas

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones a través de proveedores con experiencia en materia de gestión tecnológica y seguridad de la información, coordina las acciones de monitorización de amenazas informáticas y vulnerabilidades sobre la infraestructura TIC de la UPIT.

Los resultados de las actividades de monitorización de amenazas informáticas deben ser utilizados por el profesional responsable del Sistema de Gestión de Seguridad de la Información para planificar acciones de mejoramiento o tratamiento de riesgos y eventos de seguridad de la información.

4.1.8. Seguridad de la información en la gestión de proyectos

En los casos en que aplique, los contratos y/o proyectos de tecnología de información estarán sujetos a evaluación de riesgos de seguridad de la información. Dentro de las acciones que se deben incluir para la gestión de riesgos en la ejecución de proyectos están:

- Identificar posibles requerimientos de seguridad de la información que deberían ser evaluados como requisitos del proyecto.
- Los contratos, convenios y proyectos que adelante la UPIT deben incluir la gestión de riesgos de seguridad de información, ciberseguridad y protección de datos. La gestión de estos riesgos se debe conducir a través de la metodología institucional de gestión de riesgos.
- Los contratos, convenios que adelante la UPIT deben incluir una matriz de riesgos de seguridad de información, ciberseguridad y protección de datos; estos riesgos deberán ser gestionados por el contratista y la UPIT a través de los lineamientos institucionales.
- Identificar riesgos asociados a derechos de propiedad intelectual y licencias de uso de tecnologías de código abierto, framework de desarrollo, módulos de terceros y requisitos de licenciamiento de uso software propietario.
- Identificar riesgos de seguridad de la información asociados a la protección de datos personales que podrían estar incluidos en el proyecto.
- Identificar riesgos de ciberseguridad asociados a tecnologías no probadas o en etapas iniciales de desarrollo.
- Suscripción de acuerdos de confidencialidad y no divulgación sobre la información a la que puedan tener acceso los contratistas y/o terceros responsables de la ejecución del proyecto.
- Cumplir con las políticas y controles de seguridad establecidos por el Sistema de Gestión de Seguridad de la Información.

- Mantener la confidencialidad de la información que manejen funcionarios, contratistas y proveedores de la UPIT involucrados en las etapas del proceso de contratación y durante las etapas de gestión y ejecución de los proyectos.

4.1.9. Inventario de activos de información

Todas las dependencias de la UPIT con la coordinación del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones deben participar en las tareas de levantamiento y actualización del inventario de activos de información definido por el Modelo de Seguridad y Privacidad de MINTIC y los instrumentos de gestión de información definidos por la Ley 1712 de 2014 de Transparencia y acceso a la información pública.

Así las cosas, las actividades de identificación, clasificación y valoración de activos de información de la UPIT se deben realizar aplicando los procedimientos definidos en el sistema integrado de gestión institucional.

Las actividades de gestión de activos de información contemplan la aplicación de las siguientes normas legales referentes a la clasificación de la información:

- 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 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".*

4.1.10. Uso aceptable de activos de información

En el tratamiento de la información generada, procesada, almacenada, transferida o transmitida por los procesos de la UPIT se deben cumplir los siguientes lineamientos:

- Las actividades que se realicen con la información que está bajo responsabilidad de la UPIT deben corresponder a las funciones o actividades asignadas a los funcionarios, contratistas y proveedores de la Entidad, de tal manera que, cualquier uso diferente debe ser explícitamente aprobado por el jefe de la dependencia responsable de la información.

- El acceso a la información de la UPIT se debe realizar utilizando el usuario de red designado al funcionario o contratista al que se le ha designado para tratar la información.
- Únicamente los usuarios autorizados pueden realizar cambios en la información que está bajo su responsabilidad.
- Todos los colaboradores de la UPIT deben preservar la integridad, confidencialidad y disponibilidad los diferentes activos de información a los cuales se les ha autorizado el acceso, asegurándose que la información a la cual tiene acceso solo sea utilizada para el desarrollo de las labores o actividades asignadas.
- Cada activo de información de la Entidad debe tener asociado un responsable que debe velar por su seguridad. Los responsables identificados deben garantizar que sus activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención.
- Se debe promover el buen uso de los activos de Información, conservando el derecho a la intimidad, la privacidad, el habeas data y la protección de los datos de sus propietarios o custodios.
- Los funcionarios y contratistas son los responsables del tratamiento de la información que se encuentra en los equipos de cómputo institucional, dispositivos móviles propios o de la Entidad, nube y documentación física para llevar a cabo sus funciones y deben abstenerse de realizar en ellos tratamiento de información no institucional.
- Los dispositivos, equipos o servicios de almacenamiento de la Entidad no podrán ser usados para archivos personales como música, vídeos, fotografías o cualquier otro que no sea para uso de institucional.
- Todos los escritorios físicos y virtuales de los funcionarios o contratistas de la Entidad se deben mantener despejados y libres de información pública reservada o pública clasificada.
- No está autorizado en ninguna circunstancia realizar las siguientes acciones:
    a. Realizar copias del software licenciado de la UPIT para uso personal.
    b. Intentar instalar software no autorizado por la UPIT, en cualquier computador o servidor de la Entidad sin autorización expresa del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.
    c. Introducir programas maliciosos en las redes o a los servidores de la UPIT (ejemplo: virus informáticos, gusanos, troyanos, spyware, adware, puertas traseras, spam, ataques DDOS, *keyloggers* o cualquier otro tipo de programa maligno).

d. Realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, fondo de pantalla y protector de pantalla institucional.

4.1.11. Devolución de activos de información

Al momento de la finalización de la relación laboral o contractual con la UPIT, el funcionario o contratista, debe realizar la devolución de todos los activos informáticos y entrega de la información a su cargo siguiendo los procedimientos definidos por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

Una vez confirmada la entrega ordenada y completa de los activos a cargo del funcionario o contratista el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones emitirá el respectivo paz y salvo de entrega de activos de información.

4.1.12. Clasificación de la información

Los activos de información de la UPIT se clasifican conforme a lo dispuesto por las siguientes normas:

- 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 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 1564 de 2012, *"por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones".*

Calificación de la información	Valor de confidencialidad	Fuente normativa
Datos de niñas, niños y adolescentes	Muy Alta	Ley 1581 de 2012 Art.7
Datos personales sensibles	Muy Alta	Ley 1581 de 2012 Art.5
Información pública clasificada	Muy Alta	Ley 1712 de 2014 Art. 6
Información pública reservada	Muy Alta	Ley 1712 de 2014 Art. 6
Dato personal privado	Alta	Ley 1266 de 2008 Art 3.

Calificación de la información	Valor de confidencialidad	Fuente normativa
Dato personal semiprivado	Alta	Ley 1266 de 2008 Art 3.
Dato personal público	Moderada	Ley 1266 de 2008 Art 3.
Documento público	Moderada	Ley 1564 de 2012, Articulo 243
Datos Abiertos	Moderada	Ley 1712 de 2014, Art 6, j.

Los resultados de la clasificación de los activos de información podrán utilizarse como criterio de asignación de acceso a la información, así como para definir los controles con el fin de proteger la confidencialidad, integridad y disponibilidad de los mismos.

4.1.13. Etiquetado de información

Los jefes de las dependencias de la UPIT pueden establecer lineamientos para el etiquetado de la información electrónica que se gestiona en sus procesos. El proceso de etiquetado de la información puede incluir inserción de marcas de agua, encabezamientos o pie de página. Las etiquetas de identificación de la información deben ser iguales a los niveles de clasificación de la información definidos en la Política de clasificación de la información institucional.

Con el apoyo del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, las dependencias realizan implementación de los controles de seguridad en las plataformas tecnológicas de almacenamiento de información para garantizar la aplicación de las etiquetas electrónicas aprobadas.

Por su parte, el área de gestión documental aplicará el etiquetado electrónico de documentos y expedientes de acuerdo con la Política Institucional de Clasificación y Etiquetado de Información.

4.1.14. Transferencia de información

Los requerimientos de información que se formulen a la UPIT por parte de las entidades estatales en cumplimiento de una función administrativa o en ejercicio de una facultad legal, o por los particulares encargados de una función administrativa, a otras entidades del Estado, no constituyen solicitud de un servicio y, por ende, no generan costo alguno para la entidad solicitante.

Para efectos del intercambio de información, las entidades estatales o los particulares que ejercen funciones públicas deben coordinar procedimientos técnicos con la UPIT para integrar, compartir y/o suministrar la información que por mandato legal se

requiere, o permitir el acceso total, dentro del marco de la Constitución y el derecho fundamental a la intimidad, a las bases de datos completas que requieran otras entidades para el ejercicio de sus funciones.

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de orientar a las dependencias de la UPIT en la definición de las condiciones técnicas de seguridad para la transmisión de información.

El intercambio de información entre entidades se deberá realizar a través de los protocolos de interoperabilidad adoptados por la UPIT.

La transmisión de la información se desarrollará teniendo en cuenta la normatividad colombiana vigente, especialmente la relativa a la Ley de Habeas Data (Ley 1266 de 2008), la Ley de Protección de Datos Personales (Ley 1581 de 2012 y decretos reglamentarios) y Ley de Transparencia (Ley 1712 de 2014).

Las condiciones para la transmisión de información deben ser documentadas formalmente y aprobadas por la parte receptora de la información y la UPIT.

Para lo anterior, será necesaria la suscripción de acuerdos de confidencialidad entre las partes que hacen la transferencia de información en caso de que la información que se transmita este sometida a reserva.

La transmisión de información reservada debe ser cifrada o realizada por canales cifrados que garanticen la confidencialidad y se tendrá registro de la transmisión realizada, el cual debe ser documentado por la dependencia responsable de la transferencia de información. El cifrado de información se debe realizar de acuerdo con las políticas de seguridad de la información de la UPIT.

4.1.15. Control de acceso a la información

El acceso a la información, los sistemas de información y demás recursos de información de la UPIT se debe realizar mediante la cuenta de acceso institucional asignada por El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

El acceso a los activos de información de la UPIT se otorga aplicando las recomendaciones de estándares de seguridad reconocidos en la Norma Técnica Colombiana ISO 27002, que consisten en:

- Necesidad de uso: una cuenta de usuario solo tendrá acceso a la información que requiere para realizar las tareas que le han sido asignadas;
- Mínimo privilegio: los privilegios de acceso se otorgan bajo el principio de mínimo privilegio, que significa, que en general todo acceso está restringido a menos que sea explícitamente autorizado.

El control de acceso a los activos de información almacenados en medios físicos (discos duros, memorias USB, archivo físico en papel) se debe realizar mediante controles de acceso físico que limiten las posibilidades de pérdida de confidencialidad, integridad o disponibilidad por parte de terceros no autorizados.

Por su parte, el control de acceso a los activos de información almacenados en medios electrónicos se debe realizar mediante controles de acceso lógico que limiten las posibilidades de pérdida de confidencialidad, integridad o disponibilidad por parte de terceros no autorizados. Los controles de acceso lógico deben cumplir con el nivel de calificación del activo de información, los roles y funciones del personal al que se le otorgará el acceso.

Solamente los responsables de los activos de información pueden solicitar el cambio o retiro de los controles de seguridad de acceso físico o lógico de los activos de información as su cargo. Los cambios en las autorizaciones de acceso a los activos de información se deben registrar y tramitar a través de la mesa de ayuda del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

4.1.16. Uso del servicio de correo electrónico

Los usuarios del servicio de correo electrónico de la UPIT deben cumplir los siguientes lineamientos de seguridad para uso del servicio:

- Usar la cuenta de correo electrónico institucional como herramienta tecnológica para el desarrollo de sus funciones u obligaciones pactadas y no para fines personales.
- Los usuarios del servicio de correo electrónico institucional son responsables de todas las actividades que se ejecuten con sus cuentas de correo electrónico.
- Dar cumplimiento a las políticas, guías y lineamientos expedidos por la Entidad y aplicación de la normativa legal vigente aplicable en aspectos como: seguridad de la información, ciberseguridad, privacidad, protección de datos, derechos de propiedad intelectual, confidencialidad y las demás normas que le sean relacionadas con el servicio de correo electrónico institucional.
- Solicitar a la mesa de ayuda la creación de una cuenta de correo electrónico institucional a través de la autorización emitida por el jefe de la dependencia en la cual se cumplen las funciones o actividades.

- Mantener la confidencialidad de sus credenciales de acceso al servicio.
- Aplicar la política de seguridad de contraseñas.
- Reportar a la mesa de ayuda fallas de seguridad, correos sospechosos o incidentes en el servicio de correo electrónico institucional.
- Se considera como uso no adecuado del correo institucional las siguientes acciones:
    a. Utilizar el servicio de correo electrónico para fines personales.
    b. Enviar mensajes o materiales de carácter ilícito, que supongan acoso, difamación, insulto o amenaza, o contenidos con códigos maliciosos.
    c. Enviar información que vulnere los derechos de autor o de propiedad intelectual u otras normativas legales aplicables.
    d. Dejar la sesión de correo electrónico abierta y disponible para el uso por parte de personas no autorizadas.
    e. Enviar deliberadamente a otros usuarios o direcciones de correo electrónico mensajes no deseados (spam), software de malicioso o códigos o archivos diseñados para producir daños a los sistemas de información, publicidad no deseada o material prohibido por las regulaciones a las que está sometida la UPIT.
    f. Registrar o iniciar sesión en sitios web o aplicaciones de servicios inseguros o sospechosos usando la cuenta de correo institucional.
    g. Modificar mensajes de correo electrónico recibidos o enviados sin el permiso del remitente o del destinatario.

4.1.17. Acceso y uso seguro de redes sociales

Para un uso seguro de las redes sociales de la UPIT, los administradores de redes sociales institucionales deben aplicar los siguientes lineamientos de seguridad:

- Las contraseñas de acceso para la administración de las redes sociales de la UPIT deben:
    a. Cumplir la política de contraseñas seguras institucional.
    b. Las claves de acceso a las redes sociales de la UPIT deben ser únicas e intransferibles, las claves de administración de uso compartido se deben realizar mediante protocolos definidos por los profesionales responsables de la administración de redes sociales.
    c. Las contraseñas de acceso a las redes sociales de la UPIT no se deben usar como contraseñas de acceso a otros sistemas o servicios de información.
    d. Se debe cambiar la contraseña de acceso a las redes sociales como mínimo cada sesenta (60) días.
    e. No se deben reciclar para uso las últimas tres (3) contraseñas de administración de la red social.

f. Se debe utilizar el doble factor de autenticación en las redes sociales que permitan habilitar este mecanismo de control.
g. Las redes sociales que admitan contraseña de primer uso para cambio en la primera autenticación deben habilitar ese mecanismo de seguridad.
h. La cuenta de correo electrónico designada como usuario para administración de las redes sociales debe ser configurada con doble factor de autenticación.
i. La cuenta de correo electrónico designada como usuario para administración de las redes sociales debe ser una cuenta de correo institucional de la UPIT. No se deben utilizar cuentas de correo electrónico de servicios gratuitos a excepción de que la red social exija el uso de sus propios correos.
j. La administración de las redes sociales institucionales desde dispositivos móviles se debe hacer desde dispositivos de propiedad de la UPIT.
k. Las autorizaciones de conexión de las aplicaciones de terceros no utilizadas o sospechosas en la red social deben ser revocadas.
l. El acceso a las páginas de administración de las redes sociales se debe realizar usando la URL oficial de la red, nunca desde vínculos en correos electrónicos, mensajes instantáneos o sitios web externos a la red social.
m. La cuenta de administración de red social se debe configurar para que notifique los inicios de sesión nuevos al administrador de la red social.
n. Las sesiones de administración de la red social que no estén activas se deben cerrar.
o. Al finalizar las labores de administración o publicación de información de la red social se debe cerrar la sesión cuando se usen equipos que no cuenten con las condiciones mínimas de seguridad para prevenir ataques informáticos.
p. Se debe configurar la cuenta de administración de red social de modo que sea obligatorio proporcionar una dirección de correo electrónico y un número de teléfono para poder solicitar un enlace o código de restablecimiento de la contraseña: opción de protección de restablecimiento de contraseña.
q. Las claves de administración de las redes sociales de la UPIT deben ser comunicadas a la Secretaría General para su custodia en caso de ausencia provisional o definitiva del (los/as) administrador(a/es) de las redes sociales de la UPIT.
r. Los computadores desde los que se realicen las tareas de administración y publicación de información en las redes sociales de la UPIT deben contar con antivirus, mantener actualizado su sistema operacional y tener habilitado el bloqueo de sesión en caso de inactividad.
s. Los dispositivos móviles desde los que se administre o publique información en las redes sociales de la UPIT deben tener actualizado su

software de sistema operacional y tener habilitada contraseña de acceso y bloqueo por inactividad.

t. Las labores de administración y publicación de información en las redes sociales de la UPIT se deben realizar desde redes seguras. Se debe evitar el uso de redes gratuitas o desconocidas para realizar las tareas de administración de las redes sociales institucionales.
u. Las cuentas de redes sociales de pago o empresariales tienen mayores niveles de seguridad, capacidad de administración y posibilidad de control de acceso a la información mediante roles de usuario, que las cuentas de red social gratuita. Por motivos de seguridad se preferirá la utilización de cuentas de red social empresarial para evitar incidentes y ataques informáticos contra la UPIT.

4.1.18. Uso seguro del servicio de acceso a Internet

El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas asignadas a los funcionarios, contratistas o proveedores responsables de la prestación de servicios para la UPIT.

Este acceso podrá ser asignado a las personas que cumplan funciones o desarrollen actividades para la UPIT, ya sea funcionario o contratista. La autorización de uso del servicio de acceso a Internet para los visitantes a las instalaciones de la UPIT debe ser solicitada por los responsables de procesos o dependencias que recibe la visita.

Los servicios de acceso a Internet que se asignen a un determinado usuario dependerán del rol y funciones que desempeña en la Entidad y para los cuales esté formal y expresamente autorizado (navegación, descarga o transferencia de archivos, acceso a redes sociales, servicios de noticias, video en línea, etc.).

El acceso a redes sociales, video en línea, audio o servicios no directamente afectos a los servicios de la UPIT, se autoriza a las dependencias cuya función misional requiere de esos servicios de Internet. La Entidad se reserva el derecho de suspender dichos servicios de acuerdo con situaciones de riesgo identificadas o reportadas.

Todos los usuarios del servicio de acceso a Internet deben informar a la mesa de ayuda los contenidos no autorizados o sospechosos identificados en la conexión a Internet.

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones puede supervisar el uso y acceso del servicio de Internet para certificar que se está usando para el cumplimiento de las funciones asignadas. En los

procesos de verificación del uso apropiado del servicio de acceso a Internet se respetan los derechos a la intimidad y privacidad de los usuarios.

El acceso a sitios web e información publicada en Internet puede ser suspendido si se identifican acciones que impliquen:

a. Riesgos de seguridad de la información, ciberseguridad y protección de datos personales.
b. Ejecución de acciones ilícitas de acuerdo con la normatividad legal vigente (Ley de delitos informáticos, ley de infancia y adolescencia)
c. Usar el servicio de acceso a Internet para actividades personales.
d. Descargar, gestionar o cargar ilegalmente contenidos protegidos por derechos de autor a través de los equipos de cómputo de la UPIT (música, videos, obras literarias, pictóricas, imágenes) sin contar con la respetiva autorización.
e. Publicación de información que afecte negativamente la imagen de la UPIT o sus servidores.
f. Publicar información basada en sus opiniones, criterios, pronunciamientos y/o posiciones personales y presentarla como si fuera compartida y autorizada por la Entidad.
g. Realizar o fomentar propaganda de productos comerciales o propaganda política.
h. Distribuir correos electrónicos y mensajes no deseados o spam a través de los equipos de la Entidad
i. Distribuir mensajes e imágenes acosadoras, violentas, discriminatorias o de odio por medio de los equipos de la Entidad.
j. Acceso a servicios de video juegos, apuestas o entretenimiento en línea;
k. Acceso a material pornográfico o a sitios Web de contenido para adultos relacionados con desnudismo, erotismo o pornografía.
l. Acceso a sitios web que fomenten la discriminación por razones raciales, políticas, ideológicas, de género o de cualquier otra índole que vayan en contravía de la constitución política de Colombia o los derechos humanos.
m. Uso comercial del servicio de acceso a Internet de la Entidad
n. Espionaje o captura no autorizada del tráfico de datos de las redes de la UPIT.
o. Ingreso a páginas relacionadas con violencia, drogas, alcohol, web proxys, hacking o cualquier sitio web que puedan implicar compromiso de seguridad de la información de la Entidad.
p. Intercambiar información de la Entidad con terceros sin previa autorización del responsable del proceso.
q. Realizar capturas de datos de acceso, contraseñas o cualquier información que circule por la red de la UPIT.

r. Descifrar cualquier tipo de información de la Entidad, como el correo electrónico, en los equipos de cómputo de la UPIT.
s. Instalar software que pueda ser per para los equipos y la red de la UPIT.
t. Ejecutar transacciones que consuman recursos informáticos en detrimento de la funcionalidad de los recursos tecnológicos de la UPIT.

Para garantizar un uso seguro de servicio de acceso a Internet todos los usuarios del servicio deben:

a. Verificar que las URL de los sitios web sean seguras e inicien con https://
b. Evitar seguir enlaces sospechosos en correos electrónicos o sitios web desconocidos.
c. Evitar grabar contraseñas en los navegadores web.
d. Habilitar el antivirus del computador durante la navegación por Internet.
e. Evitar instalar software, módulos o librerías anunciados por la página web visitada y que se sospeche sean inseguros o no haya sido verificados previamente por la mesa de ayuda de la UPIT.

4.1.19. Gestión de la seguridad y calidad de los datos

Los datos e información de la Entidad deben ser asegurados, previniendo pérdidas o daños derivados de su uso indebido, para ello: deben ser protegidos mediante acciones que permitan la planificación, implementación y mantenimiento de controles seguridad políticas y procedimientos para proporcionar autenticación, autorización, acceso, y auditoría de datos y activos de información.

Las políticas y procedimientos de seguridad de la información de la UPIT deben asegurar que solo las personas debidamente autorizadas puedan usar y actualizar los datos en la forma correcta e impedir el acceso inapropiado y cambios no autorizados.

En los procesos de gestión de la seguridad de la información para la calidad de los datos de la UPIT se aplican principios de calidad, seguridad y gobierno de datos que contemplan las siguientes acciones:

- Los datos se deben clasificar de acuerdo con las normales legales vigentes de protección de datos personales, transparencia y acceso a la información pública y la normatividad que determinan reserva de la información. Los datos de la UPIT se clasifican de acuerdo con la Política de Clasificación de Información Institucional.
- De acuerdo con su nivel de clasificación el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y Comunicaciones define las medidas

tecnológicas de protección necesarias para prevenir la perdida de confidencialidad, integridad y disponibilidad.

- Los jefes de dependencias deben identificar el uso autorizado de los diferentes tipos de datos en los distintos procesos de la Entidad.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y Comunicaciones deben determinar los requisitos de seguridad de la información que deben cumplir los procesos estratégicos, misionales, de apoyo, y de evaluación y mejora para la protección de la integridad, confidencialidad y disponibilidad de los datos que gestionan.
- Los jefes de las dependencias deben determinar los roles y permisos de seguridad de la información que se asignen a los funcionarios, contratistas y partes interesadas responsables de prestación de servicios.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y Comunicaciones debe definir e implementar los controles y procedimientos de seguridad de la información que se aplican en las actividades de recolección, almacenamiento, procesamiento y comunicación de datos.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y Comunicaciones debe definir los lineamientos para la monitorización de las acciones realizadas por los usuarios con los diferentes tipos de datos.

4.1.20. Gestión de identidades y cuentas de usuario

La asignación de cuenta de usuario para acceso a los activos de información de la UPIT debe ser solicitada por el jefe de la dependencia de la persona a la que se asignará la cuenta de usuario. Las solicitudes de cuentas de usuario se realizan a través de la mesa de ayuda UPIT.

Lo anterior de acuerdo con los siguientes lineamientos:

- Cada cuenta de usuario se asigna a una única persona con la debida asignación de sus derechos de acceso.
- Las cuentas de usuario para acceso a los activos de información, servicios tecnológicos y sistemas informáticos de la UPIT son personales e intransferibles.
- La asignación de cuentas de usuario compartidas que son gestionadas por varias personas solo se permite por razones asociadas al cumplimiento de las funciones o actividades y autorizadas por el superior inmediato de las personas que gestionarán la cuenta compartida.
- Al momento del retiro del funcionario o contratista responsable de la cuenta, se hará la desvinculación de la cuenta de usuario asignada y de igual forma se ajustan los derechos de acceso de las cuentas de los usuarios en los casos que sea necesario aplicar.

- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones mantiene un registro de los responsables de las cuentas de usuario y las cuentas con derechos de acceso privilegiado para lograr un control de acceso a la información a través de las cuentas asignadas.
- Las cuentas de usuario con privilegios de administrador de activos de información (servidores, servicios, bases de datos, sistemas de información) deben tener habilitado el registro de los eventos ejecutados con la cuenta de usuario.
- La UPIT se adhiere a los lineamientos de seguridad de autenticación de usuarios de los servicios informáticos suministrados por terceros y sobre los cuales no se tiene control y/o privilegios de administrado, por ejemplo: redes sociales, SECOP, Colombia Compra Eficiente, SIIF nación.

4.1.21. Información de autenticación y claves de acceso

La información de autenticación que corresponde a la clave o contraseña para la cuenta de usuario es personal e intransferible.

La utilización de contraseñas de usuario debe cumplir con la Política de Contraseña Segura, así:

- Los usuarios no deben escribir sus contraseñas en lugares inseguros o expuestos a la vista.
- Los usuarios pueden utilizar software especializado para generar y almacenar sus contraseñas. El Grupo Interno de Trabajo de Gestión de Tecnologías de Información y las Comunicaciones asesora a las dependencias y usuarios en el tipo de software apropiado para almacenar las contraseñas.
- Los usuarios deben cambiar sus contraseñas cada treinta (60) días.
- No se deben reutilizar las últimas tres (3) contraseñas.
- Los usuarios deben crear sus contraseñas con mínimo 8 caracteres con las siguientes características:

    a. Que contenga letras mayúsculas.
    b. Que contenga letras minúsculas.
    c. Que contenga números.
    d. Que contenga caracteres especiales (#$%@/).
    e. Que no tengan relación con el nombre propio, familiares, cargo de trabajo o información personal que sea de fácil identificación

- Los usuarios deben cambiar la contraseña siempre que haya indicio de puesta en peligro del sistema.

- No se deben usar las mismas contraseñas para propósitos institucionales y para propósitos personales.
- Se puede cambiar la contraseña en cualquier momento, no hay restricciones sobre el periodo mínimo de uso de la contraseña.
- Las claves de acceso para autenticación de cualquier cuenta de usuario que sea afectada, comprometida o conocida por terceros no autorizados se deben cambiar a la mayor brevedad posible.
- El uso de técnicas o herramientas para obtener sin autorización la información de autenticación de usuario es un incidente de seguridad de la información que se gestiona mediante los procedimientos del Sistema de Gestión de Seguridad de la Información de la UPIT.
- La información de autenticación para las cuentas de usuario asignadas a servicios informáticos como conexiones de bases de datos, servidores de páginas web, servicios de monitorización y en general cuentas de usuario que son gestionadas directamente por el sistema operativo de los servidores y solo debe ser conocida por el personal que administra esos servicios informáticos.
- La contraseña, clave, pin o pregunta de seguridad asignada a las cuentas de usuario proporcionados por terceros a la UPIT como: redes sociales, servicios de información como SECOP, SIIF, Colombia Compra Eficiente, plataformas de administración de servicios como correo o servicios de nube, debe cambiarse cuando se utilice la cuenta por primera vez.
- Los responsables de la administración de las cuentas de usuario asignadas por terceros a la UPIT deben establecer los controles de protección de la información de autenticación incluyendo: contraseñas de usuario seguras, configuración de doble factor de autenticación cuando esté disponible, cambio periódico de claves, impedir la reutilización de claves y otros controles recomendados o exigidos por el tercero que gestiona el servicio.

4.1.22. Derechos de acceso

La UPIT está comprometida con la preservación de la confidencialidad, integridad y disponibilidad de los activos de información que son accedidos o se encuentran a cargo de sus funcionarios o contratistas. Por tal motivo la UPIT ha establecido controles que permiten regular el acceso a las redes, datos e información, así como la implementación de perímetros de seguridad para la protección de las instalaciones, especialmente, aquellas clasificadas como áreas seguras, como los centros de procesamiento de información, áreas de almacenamiento de información física, cuartos de suministro de energía eléctrica, aire acondicionado, entre otras.

- El acceso a la información y sistemas de información debe ser controlado conforme a los roles y responsabilidades de los funcionarios y contratistas. La autorización de acceso a sistemas de información debe ser otorgada por los

responsables de los activos de información o coordinador de esta dependencia. La creación de cuentas de usuario se gestiona a través de la mesa de ayuda de la UPIT.

- Todos los usuarios tendrán un usuario personal e intransferible, que permitirá los acceso y uso de la información. Todas las acciones realizadas con el usuario asignado serán responsabilidad del funcionario o contratista o tercero a quien se le asignó el usuario.
- Los permisos de acceso de un usuario o aplicativo en un sistema de información deben ser autorizados previamente por el jefe de la dependencia en la que trabaja la persona, el líder del proceso o el responsable del sistema de información.
- Todos los permisos de acceso a sistemas de información deben cumplir el principio de mínimo privilegio necesario para la realización de las funciones del usuario o el funcionamiento del aplicativo.
- Los responsables o encargados de los activos de información o sistemas de información son responsables de realizar revisiones periódicas de los derechos de acceso de los usuarios de sus sistemas de información. El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones apoya a las dependencias en las actividades de verificación de permisos de acceso a los activos de información.
- Los responsables o encargados de los activos de información periódicamente deben verificar los niveles de acceso (o también llamados niveles de privilegios) asignados a los usuarios, para garantizar que sean apropiados de acuerdo con el propósito institucional y se conserve la separación de funciones. Para el caso de los contratistas, esta verificación se realizará anualmente o por cambio de contrato.
- Una vez se apruebe el acceso a la información, los funcionarios y contratistas no deben realizar modificaciones sobre la información sin la debida autorización, deben guardar confidencialidad de la información a la cual tiene acceso y no vulnerar los controles de seguridad establecidos por la UPIT.
- Los funcionarios, contratistas y terceros de la UPIT tienen como responsabilidad velar por la integridad, confidencialidad y disponibilidad de la información, los activos y los sistemas informáticos a los que les haya otorgado acceso, asegurándose que estos solo sean utilizados para el desarrollo de las labores encomendadas.
- Como responsables de la información, los funcionarios y contratistas de la UPIT deben administrar y hacer cumplir los lineamientos de control de acceso a la información establecidos, con el fin de evitar accesos no autorizados, pérdidas o utilización indebida de los activos de información.
- La UPIT mantiene el control de acceso a la información teniendo en cuenta tanto el control de acceso lógico como el control de acceso físico. De acuerdo con el nivel de clasificación de la información se mantienen registros que

permiten garantizar la trazabilidad de las acciones realizadas, identificando, entre otros datos relevantes: quién realiza el acceso, las operaciones ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso, accesos denegados. Los registros de acceso y actividades desarrolladas podrán ser auditadas para propósitos de control e investigación de eventos o incidentes de seguridad de la información, y así mismo para minimizar el riesgo de la pérdida de integridad o confidencialidad de la información.

- La información de naturaleza pública de la UPIT debe de estar disponible al ciudadano siempre y cuando no esté sometida a reserva legal o existan restricciones para su acceso.
- Los accesos tanto físicos como lógicos, asignados a los funcionarios, contratistas y terceros deberán ser desactivados o modificados una vez terminados los vínculos contractuales con la UPIT.
- La UPIT establece controles para restringir accesos a áreas seguras, entre otros: llevar un registro de las personas que ingresar a las áreas seguras como centros de datos, centros de cableado, almacén de archivo o bodegas de almacenamiento de equipos.

4.1.23. Política de seguridad para relación con proveedores

Los proveedores de servicios y productos para la UPIT deben cumplir las Políticas de Seguridad de Información y Protección de Datos Personales de la Entidad y Deben comunicar al Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, el protocolo o mecanismos que aplican para la gestión de incidentes de seguridad de la información.

Cuando se requiera otorgar acceso a los activos de información a los proveedores de la UPIT, el responsable del activo, con apoyo del responsable de seguridad de la información de la Entidad, deben realizar un análisis de riesgos con el fin de determinar los controles de seguridad que preserven la confidencialidad, disponibilidad e integridad, así como la finalidad del uso de los datos y el respectivo consentimiento en los casos que aplique conforme a los procedimientos legales y administrativos.

Los proveedores de proyectos para la UPIT deben cumplir con la Política Institucional de Seguridad para Proyectos.

4.1.24. Acuerdos de confidencialidad con Proveedores

Antes de conceder los permisos de acceso a la información de la UPIT, el responsable del activo debe definir: las necesidades del acceso, el acceso requerido (físico o lógico), el nivel de clasificación de la información a acceder, la finalidad de uso, los

controles mínimos para tener en cuenta frente al tratamiento de la información y el manejo de incidentes de seguridad de la información.

En ningún caso se otorgará acceso a la información, sistemas de información o áreas seguras de la UPIT a proveedores, hasta no haber realizado la adecuada gestión de los riesgos, formalizado la relación contractual. El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones apoya a las dependencias en la identificación de riesgos y controles de seguridad cuando se requiere otorgar acceso a la información de la UPIT a proveedores u otras entidades.

Los contratos o convenios firmados por la Unidad, deben incluir acuerdos de confidencialidad y no divulgación de la información que definan claramente los requerimientos de seguridad y privacidad tales como: información a tratar; niveles de clasificación; finalidad; autorizados para el tratamiento; controles a tener en cuenta antes, durante y después del tratamiento de los datos por parte del proveedor, con el respectivo consentimiento por parte de los titulares en los casos que aplique; así como las responsabilidades de las partes conforme a los lineamientos de la UPIT y la legislación vigente.

Los proveedores de la UPIT deben comunicar al Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones el protocolo o procedimiento que aplican para gestionar los cambios en la prestación de los servicios que suministran (ventanas de mantenimiento, actualización de equipos, cambios en el software), así como el protocolo o plan de manejo de emergencia o gestión de la continuidad de los servicios contratados.

El responsable del activo de información no debe permitir el acceso a la información hasta no tener firmados y formalizados, por medio de un contrato o acuerdo con los proveedores, los fines de uso, condiciones de tratamiento, así como la debida implementación de los controles requeridos para preservar las características de confidencialidad, integridad y disponibilidad de la información.

Antes de brindar acceso a los activos de información, los proveedores deben aceptar formalmente el cumplimiento de las políticas de seguridad y privacidad de la información de la UPIT.

4.1.25. Gestión de seguridad la información en la cadena de suministro

Las actividades de suministro, entrega y logística de equipos deben seguir los lineamientos de seguridad definidos por los proveedores de equipos para la UPIT.

- La entrega de servicios o productos por parte de proveedores debe garantizar las condiciones de seguridad necesarias para identificar de manera segura al personal que realice la recolección o entrega de equipos y/o servicios en la UPIT.
- Todos los equipos informáticos que sean recibidos en las instalaciones de la UPIT deben seguir el protocolo de inspección definido por la compañía de vigilancia del edificio en donde se ubican las oficinas de la Entidad.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de verificar las especificaciones técnicas y de seguridad de los equipos que sean entregados a la UPIT.
- Los proveedores deben entregar los equipos a la UPIT en áreas vigiladas y controladas, evitando el acceso no autorizado a las áreas de procesamiento y almacenamiento de información de la Unidad.
- Antes de su recepción formal por parte de la UPIT se debe verificar que los equipos cumplan con las características técnicas y de seguridad pactadas con el proveedor.

4.1.26. Seguimiento y control de cambios de servicios de proveedores

Los cambios sobre las instalaciones de procesamiento de datos, servicios tecnológicos y sistemas de información se deben controlar a través de los mecanismos de gestión de cambios definidos por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

Los cambios sobre los sistemas de información se deben gestionar durante la totalidad de su ciclo de vida: especificación, diseño, prueba, puesta en producción, retiro definitivo. En las diferentes etapas y de acuerdo con la necesidad se deben mantener documentación de las acciones y cambios realizados.

Los cambios en los ambientes de producción y pruebas deben incluir actividades de evaluación de los riesgos de seguridad de la información. Cuando los cambios correspondan a desarrollo de software el proveedor debe cumplir la Política de Desarrollo Seguro de la UPIT.

4.1.27. Seguridad de servicios de nube

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones define los mecanismos de control y gestión de riesgos de seguridad de información y ciberseguridad requeridos, a los proveedores de servicios de nube de la UPIT y orienta las actividades que permiten comprobar que estos proveedores cuenten con los controles administrativos y técnicos necesarios para lograr el

cumplimiento de los requisitos legales y estatutarios en materia de seguridad de la información, ciberseguridad y protección de datos personales.

Los lineamientos sobre las responsabilidades en materia de seguridad de la información para los servicios de procesamiento y almacenamiento en nube de la UPIT deben estar alineados con las recomendaciones y buenas prácticas formuladas por el Cloud Security Alliance https://cloudsecurityalliance.org/

En la adquisición de servicios de nube, bajo la modalidad denominada software como servicio (SaaS), la parte interesada responsable de la prestación del servicio será encargada y responsable de la implementación de los controles de seguridad de la información, ciberseguridad y protección de datos personales, la UPIT solo es responsable de acceder y administrar el uso de la aplicación instalada en la nube del proveedor del servicio.

En la adquisición de servicios de nube en la modalidad de plataforma como servicio (PaaS Platform as a Service), el proveedor de servicios en la nube será encargado y responsable de la seguridad de la plataforma, la UPIT es responsable de la seguridad de la información, ciberseguridad y protección de los datos personales de los servicios que se desplieguen sobre la plataforma provista por el proveedor del servicio.

En la adquisición de servicios de nube de servicios en la modalidad de infraestructura (*IaaS Infraestructure as a Service*) como servicio, el proveedor será encargado y responsable de la seguridad de la infraestructura base, la UPIT es responsable de la seguridad de la información, ciberseguridad y protección de los datos personales de todo lo que se construye sobre la infraestructura del proveedor de servicios.

Los servicios de nube deben contar con modelo de gestión de continuidad de operaciones y con un modelo de gestión de identidades y asignación de privilegios de la plataforma de servicios, verificando que contemple como mínimo:

- Seguridad perimetral
- Autenticación de clientes
- Gestión de acceso de las cuentas de usuario (identidad, privilegios)
- Registro, monitorización y alertas

Los servicios de nube deben contar con un modelo de respuesta ante incidentes de seguridad de la información del proveedor de servicios de nube y con un modelo de seguridad de aplicaciones del proveedor de servicios de nube, el cual debe contemplar entre otros:

- Línea base de seguridad

- Gestión de entornos aislados
- Gestión de máquinas virtuales independientes
- Gestión de elasticidad del servicio
- Modelo de despliegue DevOps
- Interfaz unificada de gestión del servicio

En los servicios de nube se deben contemplar aspectos de migración y eliminación segura de la información cuando finaliza la contratación del servicio.

4.1.28. Preparación y planificación de la gestión de incidentes de seguridad de la información

Con el fin de lograr respuestas rápidas, eficaces, coherentes y ordenadas ante posibles incidentes de seguridad de la información, El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, define y aplica el procedimiento de gestión de incidentes de seguridad de la información que contempla acciones para la preparación y planificación de las respuestas ante eventos de seguridad de la información no deseados que puedan afectar la seguridad de la información, la ciberseguridad y la protección de los datos personales en la UPIT.

Para realizar el tratamiento de los incidentes de seguridad de la información, la UPIT aplica el Procedimiento de Gestión de Incidentes de Seguridad de la Información.

Las actividades para gestión de incidentes de seguridad de la información, ciberseguridad y protección de datos personales contemplan:

- Planificación de la respuesta a incidentes de seguridad de la información, ciberseguridad y protección de datos personales.
- Detección de incidentes de seguridad de la información, ciberseguridad y protección de datos personales.
- Evaluación de incidentes de seguridad de la información, ciberseguridad y protección de datos personales.
- Respuesta ante incidentes de seguridad de la información, ciberseguridad y protección de datos personales.
- Gestión de lecciones aprendidas incidentes de seguridad de la información, ciberseguridad y protección de datos personales.

4.1.29. Detección y Evaluación de incidentes de seguridad de la información

Todos los funcionarios, contratistas, proveedores de servicios y partes interesadas en los servicios de la UPIT deben reportar a través de la mesa de ayuda del Grupo Interno

de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, los eventos de seguridad de la información que puedan comprometer la confidencialidad, integridad o disponibilidad de los activos de información, así como las posibles debilidades identificadas en los controles de seguridad que protegen a los activos de información.

4.1.30. Evaluación de incidentes de seguridad de la información

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones a través del responsable de seguridad de la información debe realizar la evaluación de los eventos de seguridad de la información para determinar cuáles serán gestionados mediante el Procedimiento de Gestión de Incidentes de Seguridad de la Información y cuáles son gestionados como solicitudes de soporte.

El coordinador del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, apoyado por el responsable de seguridad de la información, establecen la necesidad de escalar el incidente de seguridad de la información ante equipos de respuesta de terceras partes, especializados en delitos informáticos o gestión de ataques informáticos como el COLCERT, CSIRT, Fiscalía o Policía Nacional.

4.1.31 Respuesta ante incidentes de seguridad

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones a través del responsable de la seguridad de la información es la dependencia encargada de coordinar las acciones de respuesta ante incidentes de seguridad de la información, ciberseguridad y protección de datos personales, las repuestas frente a los incidentes de seguridad de la información se deben realizar aplicando el Procedimiento de gestión de incidentes de seguridad de la información, de evaluar la posible recolección de evidencias forenses sobre el incidente y recomendar a la Secretaría General de la UPIT la solicitud de levantamiento de información forense ante la autoridad competente.

La Secretaría General de la UPIT es la dependencia encargada de formular ante la autoridad competente la denuncia de los incidentes de seguridad de la información que constituyan delitos informáticos según la legislación vigente.

4.1.32 Recopilación de evidencias

La recolección de evidencias forenses de los incidentes de seguridad de la información debe ser realizada por la autoridad competente, quienes cuentan con el personal certificado en el manejo de la cadena de custodia de las evidencias, herramientas

certificadas para la adecuada recolección y preservación de las evidencias forenses y los métodos legalmente aprobados para presentar las evidencias en caso de denuncia formal de delitos informáticos.

4.1.33 Gestión de lecciones aprendidas

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de coordinar la recopilación de la información sobre los incidentes de seguridad de la información para preparar los reportes oficiales e identificar oportunidades de mejora y lecciones aprendidas sobre el tratamiento de incidentes de seguridad de la información, ciberseguridad y protección de datos personales.
Las lecciones aprendidas de la gestión de incidentes de seguridad de la información pueden incluir entre otros:

- Causas de los incidentes y mecanismos para prevenir su recurrencia.
- Desempeño de los equipos técnicos y directivos que participan en la gestión de los incidentes.
- Reevaluación de los riesgos de seguridad de la información.
- Reevaluación de los controles de seguridad de la información implementados.
- Reevaluación de las políticas de seguridad de la información.
- Necesidades de capacitación del personal de la UPIT frente a eventos de seguridad de información.

4.1.34 Incidentes de seguridad de la información asociados a protección de datos personales.

Conforme con lo dispuesto por los artículos 17 y 18 de la Ley 1581 de 2012 *"por la cual se dictan disposiciones generales para la protección de datos personales"* y el Titulo V Capítulo Segundo de la Circular Única de la Superintendencia de Industria y Comercio, la Secretaría General de la UPIT es la dependencia responsable de ordenar el reporte de incidentes de seguridad de datos personales en el aplicativo dispuesto en la página web de la Superintendencia de Industria y Comercio o mediante cualquiera de los canales habilitados por la SIC para recibir comunicaciones.

Los incidentes de seguridad de la información asociados a protección de datos personales se deben reportar dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

De acuerdo con lo establecido por el Titulo V Capítulo Segundo de la Circular Única de la Superintendencia de Industria y Comercio, la información relacionada con las

medidas de seguridad, los reclamos presentados por los titulares y los incidentes de seguridad reportados en el Registro Nacional de Bases de Datos no estará disponible para consulta pública.

4.1.35 Continuidad de los servicios de seguridad de la información

La gestión de la continuidad del servicio de seguridad de la información en la UPIT contempla todas las acciones necesarias para identificar los riesgos e incidentes que potencialmente puede impedir que los controles y servicios de seguridad de la información que presta el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones se puedan ver afectados generando incidentes que afecten la confidencialidad, integridad y disponibilidad de la información institucional.

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones en coordinación con las demás dependencias de la UPIT realiza los análisis de impacto a la continuidad de los servicios de seguridad y sus resultados del análisis son utilizados para determinar oportunidades de mejora y prioridades en la implementación de acciones de contingencia en caso de fallas en la prestación de servicios de seguridad de la información.

Adicionalmente, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones identifica los requisitos y controles de seguridad que se deben aplicar en caso de interrupción de servicios de seguridad de la información y en coordinación con las demás dependencias de la UPIT orienta la ejecución de las pruebas y activación de los planes de continuidad de las operaciones de seguridad de la información.

4.1.36 Preparación de las TIC frente a perdidas de continuidad de servicios

La preparación de las TIC frente a pérdidas de continuidad de servicios, contempla todas las acciones necesarias para identificar, planificar, implementar, monitorizar, evaluar y mejorar continuamente los planes de respuesta institucionales frente a incidentes que afecten la continuidad en el funcionamiento de los sistemas de información, servicios tecnológicos e infraestructura de tecnología de información y comunicaciones que soporta los servicios de la UPIT.

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones en coordinación con las demás dependencias de la UPIT participa en el diseño de los planes de mejoramiento de las capacidades en materia de continuidad y resiliencia de servicios tecnológicos para lograr su recuperación oportuna y reducir los impactos de indisponibilidad de servicios institucionales.

La definición e implementación del Plan de Continuidad de TI, el cual hace parte integral del Plan de Continuidad de Negocio (BCP) de la Entidad debe contemplar la creación de procedimientos y la implementación de controles, que mantienen disponibles los servicios tecnológicos de la UPIT en caso de incidentes mayores o situaciones calificadas como desastre.

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia que lidera la planificación, diseño, construcción, implementación, prueba, evaluación, mantenimiento y mejora del Plan de recuperación ante desastres tecnológicos de la UPIT y además evalúa y prueba la efectividad de los controles definidos en el Plan de Continuidad de TI establecido e implementado, con el fin de identificar oportunidades de mejora al desempeño, buscando siempre el cumplimiento de los objetivos de continuidad de la Entidad

La estrategia de Continuidad de Servicios tecnológicos de la UPIT incluye las fases de prevención, respuesta y manejo de incidentes disruptivos, recuperación, y restauración de la operación.

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones junto con la Secretaría General son las dependencias que definen y mantienen los canales de comunicación administrativo y técnicos adecuados hacia los funcionarios, contratistas, proveedores y partes interesadas, con el fin de responder de manera efectiva ante los eventos catastróficos.

4.1.37 Requisitos legales reglamentarios y contractuales de seguridad

Para lograr un apropiado cumplimiento de la reglamentación legal a la cual está sometida la UPIT, la entidad cuenta con una Política de Prevención de Daño Antijurídico.

A través del normograma institucional la UPIT identifica las leyes, decretos, normas y en general todas las obligaciones legales en materia de seguridad de la información.

Cuando se presentan cambios en las obligaciones legales en materia de seguridad de la información que son aplicables al LA UPIT, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones a través del responsable de seguridad de la información identifica los cambios y coordina la actualización del normograma con los responsables del sistema Integrado de gestión de la calidad.

Los requisitos legales en materia de seguridad de la información deben ser considerados dentro del análisis del contexto interno y externo de seguridad de la información.

Por medio de la declaración de aplicabilidad de controles de seguridad de información, el responsable de seguridad de la información del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones documenta las acciones necesarias para dar cumplimiento a los requisitos legales en materia de seguridad de la información.

4.1.38 Derechos de propiedad intelectual

La UPIT declara que está sometida a las normas vigentes en materia de propiedad intelectual, particularmente, a lo dispuesto en la Ley 23 de 1982, la Decisión 391 de 1993 de la Comunidad Andina de Naciones, los tratados internacionales en materia de derechos de autor, la Decisión 486 de 2000 en materia de propiedad industrial, y las demás normas que los modifican o adicionan.

A través del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones la UPIT identifica los procedimientos apropiados para cumplir los requisitos, legales y contractuales del material sujeto a protección de derechos de propiedad intelectual incluidos softwares, material bibliográfico y audiovisual.

El software solo debe adquirirse a través de fuentes legales y siguiendo los procedimientos del proceso de adquisición de bienes y servicios del Sistema Integrado de Gestión y teniendo en cuenta los siguientes aspectos:

- El material bibliográfico y audiovisual utilizado en publicaciones, sitios web, redes sociales y demás canales de comunicación institucionales deben contar con las autorizaciones de derecho de autor.
- Todo el software que sea desarrollado por o para la UPIT debe ser registrado en los inventarios de la Entidad.
- Los desarrollos de software contratados por la UPIT deben ser registrados a favor de la Entidad ante la Dirección Nacional de Derechos de Autor.
- El personal de la UPIT contratado para el desarrollo de obras científicas, culturales, desarrollo de software o cualquier material sujeto a protección de derechos de autor debe suscribir la respectiva sesión de derechos patrimoniales de acuerdo con lo establecido en el artículo 91 de la Ley 23 de 1982.
- La UPIT es titular de los derechos patrimoniales sobre las creaciones literarias y artísticas, tales como las descritas en el artículo 2 de la Ley 23 de 1982 y artículo 1 del Decreto 1360 de 1989, cuando sean producidos por un servidor, contratista, tercero en los casos en los cuales tales obras sean:

a. Producidas por servidores vinculados.
b. Realizadas por contratistas y terceros como parte de sus obligaciones contractuales y funciones para los cuales fueron contratados.
c. Producto de investigación o creación, en la ejecución de contratos o convenios, firmados con la UPIT, específicos para la elaboración de obras científicas, literarias, artísticas o software.
d. Coordinadas, divulgadas, publicadas y/o editadas por la UPIT.
e. Los derechos sobre las obras le hayan sido cedidos de manera total o parcial a la UPIT.
f. Los derechos sobre las obras hayan sido adquiridos mediante sucesión o legado por causa de muerte

- Todo el software utilizado por la UPIT debe contar con su respectiva licencia de uso incluido el software comercial y el software de código abierto.
- El control del número de licencias de uso del software autorizado para uso en los equipos informáticos de la UPIT es responsabilidad del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.
- Anualmente el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones debe actualizar el inventario de software instalado en los diferentes equipos informáticos de la UPIT para verificar el cumplimiento de las condiciones legales de uso del software que corresponde a la cantidad de licencias, versiones y condiciones de uso.
- Las licencias del software que se dan de baja por obsolescencia deben ser registradas de acuerdo con los procedimientos de gestión de activos del Sistema Integrado de Gestión Institucional.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones en coordinación con la Secretaría General son las dependencias responsables de orientar a la UPIT en los controles y procedimientos legales para el uso legal de material protegido por derechos de autor como lo son audios, videos, imágenes, obras literarias, científicas y artísticas.
- El incumplimiento de los requisitos legales y contractuales en materia de protección de derechos de autor es un incidente de seguridad de la información, que se gestiona mediante el procedimiento de gestión de incidentes de seguridad de la información.

4.1.39 Protección de registros de auditoria

Los dispositivos y servicios tecnológicos con capacidades para generar registros de los eventos de seguridad (logs por su término en inglés) se deben configurar para producir dichos registros.

Los registros de auditoría que sean generados por los diferentes dispositivos o servicios tecnológicos se deben proteger contra acceso no autorizado o alteración.

Los registros generados por los diferentes dispositivos y servicios deben ser protegidos de acuerdo con la política de respaldo de información del Sistema de Gestión de Seguridad de la Información.

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones en coordinación con el administrador del dispositivo o el servicio tecnológico determinarán el periodo de retención de los registros de eventos que puedan ser generados y almacenados por los activos de información, en la determinación del periodo de retención de registros se tendrán en cuenta los requisitos legales a los que está sometida la UPIT.

La hora de los sistemas de información, dispositivos de comunicaciones, dispositivos de seguridad, estaciones de trabajo y en general cualquier dispositivo electrónico con capacidad de generar registro de eventos debe estar sincronizada con la hora legal colombiana establecida por el Instituto Nacional de Metrología, reglamentado en los artículos 1 y 2 del Decreto 2707 de 1982 *"por el cual se adopta la hora legal en el territorio nacional".*

4.1.40 Privacidad y Protección de los datos personales

La protección de datos personales en la UPIT debe cumplir las obligaciones de las siguientes normas legales:

a. 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".*
b. Ley 1581 de 2012, *"por la cual se dictan disposiciones generales para la protección de datos personales".*
c. Decreto 1743 de 2016, Decreto Único del Sector Administrativo de Información Estadística, art. 2.2.3.1.1 Anonimización de microdatos.

La UPIT implementa los controles de seguridad de la información definidos por la Ley 1581 de 2012 y sus decretos reglamentarios incluidas políticas, controles y procedimientos de seguridad que se deben aplicar para la preservación de la confidencialidad, integridad, disponibilidad y privacidad de los de los datos personales.

Los incidentes de seguridad de la información asociados a datos personales son gestionados por la Secretaría General de la UPIT con el apoyo del Grupo Interno de Trabajo Gestión de Tecnologías de la Información y las Comunicaciones.

Conforme con lo dispuesto en los artículos 17 y 18 de la Ley 1581 de 2012 y el Titulo V, Capítulo Segundo de la Circular Única de la Superintendencia de Industria y Comercio, la UPIT debe reportar en el aplicativo dispuesto en la página web de la Superintendencia de Industria y Comercio o mediante cualquiera de los canales habilitados por la SIC para recibir comunicaciones, los incidentes de seguridad de la información asociados a protección de datos personales dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

De acuerdo con lo establecido por y el Titulo V, Capítulo Segundo de la Circular única de la Superintendencia de Industria y Comercio la información relacionada con las medidas de seguridad, los reclamos presentados por los Titulares y los incidentes de seguridad reportados en el Registro Nacional de Bases de Datos no estará disponible para consulta pública.

De acuerdo con el nivel de riesgo identificado para los activos de información calificados como datos personales sensibles información de niños, niñas y adolescentes, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones recomendará técnicas de anonimización y cifrado de información que se deben aplicar a esos activos de información.

Cuando la UPIT determine que ciertos conjuntos de datos pueden contribuir a la generación de valor social y económico y los mismos se pueden hacer públicos se deben aplicar técnicas de anonimización para que se respeten los derechos de las personas frente a su privacidad y protección de datos personales.

Los activos de información que estén calificados como información sensible en los términos establecidos en el artículo 5 datos sensibles de la Ley 1581 de 2012 y la información de niños, niñas y adolescentes, debe ser identificada de manera visible, clara, precisa y de fácil reconocimiento para todas las personas que intervengan en el tratamiento de ese tipo de datos.

Las dependencias que tengan bajo su responsabilidad el uso y custodia de datos de carácter personal determinarán con el apoyo del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones los mecanismos que se deben aplicar para identificar los activos de información calificados como reservados, datos sensibles o información de niños, niñas y adolescentes.

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones debe recomendar los mecanismos de seguridad que se deben aplicar a los activos de información calificados como datos sensibles o información de niños, niñas y adolescentes.

En el manejo o tratamiento de datos personales de sistemas de videovigilancia y control de acceso biométrico se debe cumplir con los requisitos de la Ley 1581 de 2012 establecidos en los artículos 5 y 6 que corresponden a datos sensibles y tratamiento de datos sensibles.

En el tratamiento de los datos de sistemas de video vigilancia se debe tener en cuenta:

- Implementar video vigilancia sólo cuando sea necesario para el cumplimiento de la finalidad propuesta, respetando la dignidad y demás derechos fundamentales de las personas
- Limitar la recolección de imágenes a la estrictamente necesaria para cumplir el fin específico previamente concebido
- Informar a los titulares acerca de la recolección y demás formas de tratamiento de las imágenes, así como la finalidad de este.
- Conservar las imágenes sólo por el tiempo estrictamente necesario para cumplir con la finalidad del sistema de video vigilancia.
- Inscribir la base de datos que almacena las imágenes en el Registro Nacional de Bases de Datos.
- El acceso y divulgación de las imágenes debe estar restringido y su tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por solicitud de una autoridad en ejercicio de sus funciones
- Si en la imagen aparece un (unos) tercero(s) Titular(es) de datos personales, se deberá contar con la autorización de dicho(s) tercero(s) para la entrega de la cinta o grabación.
- Si no se tiene la autorización de los terceros para divulgar la información contenida en la cinta o grabación requerida, los responsables y Encargados del Tratamiento deben garantizar la anonimización del (los) dato (s) del (los) tercero (s), tomando medidas como hacer borrosa o fragmentar la imagen de dicho (s) tercero (s).

4.1.41 Transferencia de datos personales

Una transferencia de datos personales, como lo indica el Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, en su artículo 2.2.2.25.1.3., corresponde a:

- *Transferencia. La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.*

La transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos está prohibida por el artículo 26 de la Ley 1581 de 2012, salvo las excepciones previstas por la citada ley.

Antes de realizar transferencias internaciones de datos, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones en coordinación con la dependencia responsable de los datos personales que se requiere transferir deben identificar riesgos y controles de seguridad de protección de datos personales.

Las transferencias de datos personales sensibles y la información de niñas, niñas y adolescentes deben implementar el uso de canales de transmisión de datos seguros y deben ser protegidos mediante cifrado antes de su transferencia.

4.1.42 Revisión independiente de la Seguridad

Periódicamente la UPIT a través del Grupo Interno de Trabajo de Planeación revisa el estado del Sistema de Gestión de la Seguridad de la Información para comprobar entre otros:

- Si el sistema de gestión de seguridad de la información cumple con los objetivos propuestos.
- Si las oportunidades de mejora en la seguridad de la información, ciberseguridad y protección de datos personales se evalúan e implementan.
- Si se han gestionado los cambios internos o externos que pueden afectar al sistema de gestión de seguridad de la información, ciberseguridad y protección de datos personales.
- Si se han implementado lecciones aprendidas derivadas del tratamiento de incidentes de seguridad de la información, ciberseguridad y protección de datos personales.

Las revisiones del estado del Sistema de Gestión de Seguridad de la Información deben ser realizadas por personal independiente al área auditada para que se garantice la objetividad en la evaluación de resultados y se deben realizar siguiendo los procedimientos de auditoría interna del Sistema Integrado de Gestión Institucional.

Los resultados de la evaluación al Sistema de Gestión de Seguridad de la Información deben ser comunicados al Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones y al Comité Institucional de Gestión y Desempeño; estos resultados deben permitir la identificación de oportunidades de mejora en la gestión de la seguridad de la información, ciberseguridad y protección de datos personales.

4.1.43 Cumplimiento de políticas, reglas y estándares de seguridad de la información

Las Políticas Técnicas de Seguridad de la Información de la UPIT se revisan en el evento que se produzcan cambios de la legislación aplicable vigente y/o cuando se produzcan cambios en procesos misionales, estratégicos y de apoyo que impacten al Sistema de Gestión de Seguridad de la Información.

Las Políticas Técnicas de Seguridad de la Información se deben revisar y ajustar cuando se presenten incidentes de seguridad de la información o eventos de seguridad que no sean gestionados adecuadamente, para lo cual, anualmente el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones realiza su revisión y actualización, cuando aplique.

Así las cosas, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones a través del responsable de seguridad de la información y los jefes de las dependencias deben velar por el cumplimiento de las políticas de seguridad de la información.

Cuando se identifiquen incumplimientos de las Políticas de Seguridad de la Información se debe aplicar el procedimiento de mejoramiento continuo del Sistema Integrado de Gestión para:

- Identificar la causa raíz del incumplimiento.
- Evaluar la necesidad de implementar acciones correctivas.
- Implementar las acciones correctivas.
- Revisar la efectividad de las acciones correctivas implementadas.

Los resultados de las revisiones de cumplimiento de las Políticas de Seguridad de la Información, las acciones correctivas y sus resultados se deben mantener de acuerdo con lo especificado en los procedimientos del Sistema Integrado de Gestión y Control Institucional.

4.1.44 Procedimientos operativos documentados

La UPIT a través del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones en coordinación con el Grupo Interno de Trabajo de Planeación, elabora, socializa y realiza la actualización de procedimientos documentados, manuales, guías, instructivos y en general documentos que describan las actividades de gestión de los componentes, servicios tecnológicos y la gestión de la seguridad de la información.

Lo anterior atendiendo los siguientes criterios:

- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones implementa controles para asegurar que las operaciones de administración de la plataforma tecnológica de la UPIT se ejecuten de manera correcta y segura en las instalaciones de procesamiento de información.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es responsable de realizar monitorización constante de la gestión de la capacidad de TI, a través del análisis y evaluación de rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información.
- Los procedimientos y responsabilidades de operación y administración de la plataforma tecnológica y de seguridad deben estar documentados, garantizando un adecuado control de cambios de conformidad con los procedimientos definidos para tal fin.
- Todo cambio que se realice sobre la infraestructura tecnológica de la UPIT para el procesamiento de la información y comunicación debe ser controlado, gestionado y autorizado adecuadamente a través del procedimiento de gestión de cambios de tecnología.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones debe garantizar que los ambientes de desarrollo, pruebas y producción, siempre que sea posible, estén separados de manera física o virtual para prevenir cambios no autorizados en los ambientes de producción institucionales.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es responsable de definir y documentar las reglas para la transferencia de software de los ambientes desarrollo hacia los ambientes de producción.
- Para lograr una gestión eficiente de los servicios tecnológicos de la UPIT, los grupos encargados del desarrollo de software implementa las siguientes acciones:
    a. Ejecutar el software de desarrollo y de producción, en ambientes o equipos separados.
    b. Separar las actividades de desarrollo y prueba, en entornos diferentes.

c. Impedir el acceso a los compiladores, editores y otros programas utilitarios en el ambiente de producción, cuando no sea estrictamente necesario su funcionamiento para la prestación de servicios.
d. Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas de información. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
e. Definir propietarios de la información para cada uno de los ambientes de procesamiento

- Para preservar la integridad y confidencialidad de los activos de información de la UPIT se deben implementar en los sistemas de información y activos de información para prevenir accesos no autorizados.
- El responsable de seguridad de la información del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones debe identificar los controles de detección y prevención para la protección contra software malicioso.

Dentro los controles de seguridad para la operación de los servicios tecnológicos la UPIT contempla:

a. Prohibir el uso de software no autorizado en los equipos o servicios de la UPIT.
b. Instalar y actualizar periódicamente software de detección y reparación de software contra código maliciosos, examinado computadores y medios informáticos, como medida de precaución y rutinaria.
c. Mantener los sistemas de información y servicios con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
d. Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
e. Verificar la presencia de software malicioso en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
f. Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
g. Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
h. Documentar las fallas en los sistemas de control de seguridad con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.
i. Preservación y protección de los registros de eventos generados por los servicios, sistemas de información y equipos informáticos de las UPIT.

4.2. Seguridad en la gestión del talento humano

4.2.1. Seguridad de la información en la selección del talento humano

La selección y vinculación de los servidores públicos de la UPIT se realiza de acuerdo con los procedimientos del Proceso de Gestión de Talento Humano que sigue los procesos de verificación de seguridad establecidos por la Comisión Nacional del Servicio Civil.
Los procesos de contratación para prestación de servicios profesionales y/o de apoyo a la gestión y/o altamente calificados, se realizan de acuerdo con el procedimiento de Gestión Contractual adoptado por la Entidad, que incluye las actividades de verificación de antecedentes y verificación de competencias.

4.2.2. Términos y condiciones del empleo

Las responsabilidades de los servidores públicos de la UPIT se definen en el respectivo Manual de Funciones y Competencias Laborales de acuerdo con el Proceso de Gestión de Talento Humano y para el personal vinculado a través de contrato de prestación de servicios, estas responsabilidades se documentan en las condiciones y términos del proceso de contratación y las obligaciones en materia de seguridad de la información pactadas en los respectivos contratos.

Las responsabilidades y deberes en cuanto a la seguridad de la información se consignan en este documento de Políticas Técnicas de Seguridad de la Información.

4.2.3. Conciencia de seguridad de la información

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de liderar el diseño e implementación del plan de sensibilización en materia de seguridad de la información a todo el personal de la Entidad, incluidos funcionarios de planta y contratistas.

Las actividades de toma de conciencia en materia de seguridad de la información se registran en el Plan de Seguridad y Privacidad de la Información el cual forma parte del Plan de Acción Institucional.

Dentro del plan de sensibilización en materia de seguridad de la información, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones incluye contenidos referentes a:

a. Políticas de seguridad de la información

b. Identificación de amenazas informáticas
c. Reporte de incidentes de seguridad
d. Beneficios de la implementación de los controles de seguridad de la información

4.2.4. Procesos disciplinarios

Para los servidores públicos y funcionarios de la UPIT, los procesos disciplinarios se realizan de acuerdo con los procedimientos definidos por la Ley 1952 de 2019, por medio de la cual se expide el Código General Disciplinario.
Cuando se presentan eventos de seguridad de la información que pueden evidenciar potenciales faltas de acuerdo con el Código General disciplinario, el Coordinador del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones aplica los procedimientos definidos en la Entidad para remitir las evidencias a la Secretaría General como control disciplinario de la UPIT.

En el caso de incumplimiento de obligaciones contractuales en materia de seguridad de la información por parte de contratistas se aplica las cláusulas pactadas en el contrato.

4.2.5. Responsabilidades después de la terminación o cambio del empleo

Los funcionarios de la UPIT que finalizan su vinculación con la Entidad siguen los procedimientos definidos en el Sistema Integrado de Gestión para devolver los activos de información, dispositivos, expedientes, carnés de identificación y demás elementos de propiedad de la UPIT antes de su desvinculación formal, para lo cual se requiere el Formato de Entrega Puesto de Trabajo y Paz y Salvo con el fin de verificar la recepción de los activos de información a cargo del colaborador.

En el caso de los contratistas, cuando se produce la finalización de la relación contractual, se verifican las cláusulas pactadas y se aplica el procedimiento dispuesto por Gestión Contractual para formalizar el cierre de la relación contractual.

Al momento de la desvinculación de los funcionarios o la finalización de relación contractual de contratistas de la UPIT el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones aplica el procedimiento de gestión de cuentas de usuario para deshabilitar los accesos a los sistemas de información, realizar las copias de respaldo y recibir los equipos informáticos asignados a los colaboradores.

4.2.6. Acuerdos de confidencialidad y no divulgación

Los funcionarios de la UPIT tienen acuerdos de confidencialidad sobre la información que tienen a su cargo, según las obligaciones del servidor público consignadas en el Código General Disciplinario (Ley 1952 de 2019).

Los contratistas y proveedores de servicios para la UPIT suscriben acuerdo de confidencialidad como parte de las obligaciones pactadas en los contratos de prestación de servicios con la UPIT.

La información sometida a reserva de acuerdo con la legislación vigente se protege siguiendo la política de control de acceso de este documento.

Los acuerdos de confidencialidad sobre la información reservada o clasificada a cargo de los funcionarios y contratistas que se retiran de la Entidad permanecen vigentes de acuerdo con la legislación que cobija a los diferentes tipos de información.

4.2.7. Trabajo Remoto

La UPIT cuenta con la modalidad de teletrabajo aprobada conforme con los requisitos legales en el marco del Sistema de Gestión de Seguridad y Salud en el Trabajo.

De esa forma, la Unidad autoriza las actividades de trabajo remoto mediante servicios de conexión por medio de redes privadas virtuales VPN. La autorización de ejecución de trabajos remotos debe ser aprobado por el jefe de la dependencia en la que labora el colaborador y la autorización de la Entidad.

Para disponer de los recursos tecnológicos que permitan el acceso remoto a sus activos de información, se debe realizar trámite a través de la mesa de ayuda con la autorización del jefe de la dependencia.

Los colaboradores de la UPIT que realicen actividades de trabajo remoto sobre los activos de información institucionales deben, garantizar el cumplimiento de las políticas técnicas de seguridad la información y la política institucional de teletrabajo.

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones a través del responsable de seguridad de la información evalúa y autoriza las solicitudes de acceso remoto a las redes de la UPIT teniendo en cuenta los siguientes aspectos:

- En caso de pérdida o hurto de equipos utilizados para conexión remota a las redes de la UPIT, el funcionario, contratista o tercero responsable del equipo debe informar de forma inmediata a través de la mesa de ayuda el evento, con

el fin de establecer las medidas de seguridad adecuadas para prevenir el acceso no autorizado desde la máquina afectada por el hurto o pérdida.

- Para tramitar las autorizaciones de acceso remoto, el jefe del área deberá diligenciar la solicitud de servicio de acceso remoto a través de la mesa de ayuda detallando el nombre del usuario, la justificación de la necesidad de conexión remota, las condiciones de horario y equipos sobre los cuales se requiere el acceso remoto.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de implementar los controles de seguridad necesarios para llevar a cabo las actividades de trabajo remoto en forma segura.

Cuando se realicen actividades de trabajo remoto los funcionarios, contratistas y proveedores de servicios de la UPIT deben:

a. Acceder a los diferentes entornos y activos informáticos, respetando la normativa vigente en materia de derechos de autor y protección de datos personales,
b. Utilizar la información a la que tenga acceso única y exclusivamente para cumplir con sus funciones designadas.
c. Cumplir con las medidas de seguridad que defina la UPIT para asegurar la confidencialidad, disponibilidad e integridad de los activos de información institucionales
d. Para garantizar la conexión segura a los activos de información de la UPIT, se debe usar el software de red privada virtual (VPN) definido por El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.
e. Tener instalado en su equipo de trabajo remoto software contra código malicioso.
f. Usar software de Ofimática licenciado y actualizado.
g. Cumplir con los requisitos y obligaciones de la política de teletrabajo institucional.

4.2.8. Informe sobre eventos de seguridad de la información

Todos los funcionarios, contratistas y los proveedores de servicios para la UPIT deben reportar a la mesa de ayuda cualquier evento sospechoso que pueda ser indicio de un incidente de seguridad de la información.

La Secretaría General a través del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable

de autorizar contacto con las autoridades y grupos especializados en materia de seguridad de la información entre otros:

- Ante la Superintendencia de Industria y Comercio cuando el incidente tiene relación con protección de datos personales.
- Ante la Fiscalía general de la Nación cuando el incidente de seguridad de la información constituye delito informático.
- Ante el centro de respuesta de incidentes la Policía Nacional (CSIRT PONAL) cuando se requiera apoyo en el tratamiento de evidencias forenses de delitos informáticos.
- Ante el Centro de Respuesta ante incidentes de seguridad de la información de la UPIT de Defensa COLCERT cuando sea necesario.
- Ante el centro de respuesta a incidentes informáticos CSIRT del MINTIC cuando se identifiquen eventos o incidentes que afecten la prestación de servicios informáticos de la UPIT.

Cuando se presenten eventos o incidentes de seguridad que implique el reporte a diferentes instancias legales la Secretaría General con el apoyo del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones establecerá el orden de notificación correspondiente.

4.3. Seguridad física y del entorno

4.3.1. Perímetros de seguridad física

Para prevenir el acceso no autorizado a las instalaciones de procesamiento y almacenamiento de información, las áreas físicas que contienen equipos de procesamiento de datos, comunicaciones, almacenamiento de archivo físico y en general áreas que sean consideradas como de acceso restringido se ubican en zonas que cuentan con muros, puertas de control de acceso biométrico o con cerradura, estas áreas deben contar con barreras físicas de control de acceso que limiten el acceso a personal no autorizado.

4.3.2. Entrada Física

Todos los visitantes de la UPIT deben anunciarse en la recepción de las instalaciones de la Entidad, en donde se coordina su autorización de ingreso.

Mediante los servicios de vigilancia de las instalaciones de la UPIT se lleva un registro de datos de cada visitante el cual incluye: nombre e identificación del visitante, fecha y hora de la visita y de acuerdo con el protocolo de la compañía de vigilancia, se

puede requerir al visitante su registro fotográfico, preservando sus derechos de habeas data.

El ingreso de un visitante a las instalaciones de la Entidad debe ser autorizado por un colaborador de la UPIT. En ningún caso un visitante puede autorizar el ingreso de otro visitante.

Los visitantes deberán ser acompañados por el colaborador de la Entidad que autorizó su ingreso, durante el tiempo que dure la visita, y específicamente cuando se accede a áreas restringidas.

El colaborador de la Entidad que autorice el ingreso de un visitante es el encargado de hacerle conocer los requisitos de seguridad y los procedimientos de emergencia.

Los dispositivos electrónicos ingresados por los visitantes, tales como portátiles, computadores, tabletas, cámaras de video o dispositivos móviles son de su entera responsabilidad mientras permanezcan dentro de las instalaciones de la UPIT.

Ningún visitante podrá ingresar a áreas restringidas de la UPIT, sin tener acompañamiento del colaborador encargado de esa área, quien tendrá bajo su responsabilidad la permanencia del visitante en la Entidad durante el tiempo que dure la visita.

4.3.3. Seguridad de oficinas e instalaciones

Todas las áreas físicas de la Entidad en las que se almacenen o mantengan provisional o permanentemente activos de información calificados como clasificados, reservados o datos personales deben tener acceso restringido y en lo posible tener los perímetros de seguridad física para su protección (paredes, puertas de acceso, controles biométricos, video vigilancia, entre otros).

Las puertas y ventanas de las oficinas de la Entidad se deben mantener cerradas cuando no esté presente personal de la Entidad. Aquellas oficinas que no tengan puerta o barreras físicas de control de acceso como paredes o divisiones deben permanecer supervisadas para prevenir acceso a personal no autorizado.

Los equipos y dispositivos que son utilizados para soportar las funciones críticas de la Entidad deben estar ubicados en áreas cuyo acceso sea restringido y esté supervisado por los sus respectivos responsables.

Adicionalmente, se debe tener en cuenta que:

- Solamente el personal debidamente autorizado podrá tener acceso al área de Gestión Documental y archivo de la Entidad.
- Las puertas de acceso a los centros de datos, cuartos de comunicaciones y áreas en donde se encuentren equipos críticos para la prestación de servicios institucionales como: planta eléctrica, UPS y sistemas de aire acondicionado deben permanecer cerradas y aseguradas para prevenir accesos no autorizados.
- Únicamente se permite el ingreso permanente al centro de datos al personal autorizado, por lo que debe existir un mecanismo que registre y controle el ingreso y salida de personas, y cualquier tipo de material a esta área.
- De ser necesario el ingreso de algún visitante al centro de datos, podrá realizarse siempre y cuando sea para actividades que no afecten o modifiquen el correcto funcionamiento de la infraestructura instalada. Los visitantes al centro de datos siempre deben estar acompañados y bajo la supervisión de una persona responsable por parte de la UPIT.
- Los registros físicos o electrónicos de ingreso al centro de datos deben ser verificados con frecuencia para identificar accesos no autorizados y confirmar que los controles de acceso funcionan correctamente.

4.3.4. Monitoreo de seguridad física

Las oficinas, instalaciones de procesamiento de datos y en general todas las instalaciones de la UPIT son monitorizadas mediante sistema de video vigilancia.

Los visitantes, funcionarios, contratistas y proveedores de servicios de la UPIT aceptan la grabación de sus imágenes con la finalidad de garantizar la seguridad física de las instalaciones y los activos de información de la UPIT.

Los responsables de las áreas de almacenamiento y procesamiento de información de la UPIT deben coordinar acciones con la compañía de vigilancia para monitorizar periódicamente las áreas de procesamiento o almacenamiento de información.

El diseño e implementación de los sistemas de la monitorización de áreas de almacenamiento o procesamiento de información debe mantenerse como información clasificada para prevenir su divulgación a personal no autorizado.

Los sistemas de video vigilancia y grabación deben cumplir con los requerimientos de Protección de Datos Personales de la ley Habeas Data (Ley 1581 de 2012).

4.4. Protección contra amenazas ambientales

Las áreas de procesamiento o almacenamiento de información de la UPIT se deben proteger contra amenazas físicas y ambientales como desastres naturales, por ejemplo: incendios, inundaciones, terremotos, explosiones disturbios civiles, contaminación por agentes tóxicos y otras amenazas causadas por el hombre sean o no intencionales.

Dentro de los controles que se deben evaluar para la protección contra amenazas ambientales están:

- Incendios: sistemas automáticos de detección, alarma y control de fuego
- Sobretensión eléctrica: sistemas de puesta a tierra y prevención de sobrevoltaje o fluctuaciones en el suministro eléctrico que afecten a las estaciones de trabajo, servidores, equipos de comunicaciones y demás activos informáticos.
- Explosivos, armas, elementos tóxicos: inspección de paquetes y vehículos para detectar la presencia de armas o explosivos que pueden ingresar a las instalaciones en donde se almacena o procesa información.
- Inundaciones: sistemas de detección de temprana de fugas de agua en pisos, paredes o techos en los centros de procesamiento de datos.
- Terremoto: plan de evacuación y manejo de emergencias, plan de recuperación ante desastres.
- Disturbios civiles: plan de evaluación y manejo de emergencias, teletrabajo.

4.5. Trabajo áreas en áreas seguras y de procesamiento de datos

Todo el personal con acceso a las áreas de procesamiento de información debe participar en las actividades de sensibilización en materia de seguridad de la información, ciberseguridad y protección de datos personales coordinadas por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

Los trabajos en las áreas de procesamiento de datos deben ser supervisadas para prevenir acciones maliciosas.

Las áreas de almacenamiento, procesamiento de información y centro de cómputo deben permanecer cerradas para prevenir acceso de personal no autorizado y deben ser supervisados mediante sistema de videovigilancia.

En ese sentido, salvo autorización expresa del Coordinador del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, los visitantes no están autorizados para tomar fotografías dentro de las instalaciones definidas como áreas seguras de la Entidad. Las áreas seguras de la UPI incluyen: centro de datos, cuartos de telecomunicaciones, áreas de almacenamiento de expediente, áreas de servicios esenciales como energía eléctrica, aire acondicionado y otras que establezca la Secretaría General de la UPIT.

4.6. Escritorio y pantalla limpios

Mientras no se encuentre en uso la información calificada como reservada o clasificada debe permanecer almacenada en lugar seguro fuera del alcance de personal no autorizado.

Las estaciones de trabajo deben activar automáticamente el bloqueo de pantalla con contraseña mientras no estén en uso y durante el tiempo que queden desatendidas se debe bloquear la sesión del equipo y las conexiones a servicios informáticos de la UPIT como correo electrónico, conexión a internet, conexiones a sistemas de información deben cerrarse para evitar que terceros no autorizados accedan a la información contenida en el computador**.** Adicionalmente, fuera de los horarios laborales, las estaciones de trabajo deben permanecer apagadas para reducir el consumo energético y prevenir el acceso remoto no autorizado.

Igualmente, fuera de los horarios laborales la información impresa y los medios de almacenamiento extraíbles deben permanecer en un lugar seguro para prevenir accesos no autorizados. Las impresiones y copias de documentos deben ser retiradas a la mayor brevedad de los dispositivos para prevenir su acceso por parte de personal no autorizado.

De igual forma se deberá tener en cuenta que:

- La información valorada como reservada o clasificada que se publique en tableros o salas de reuniones se debe retirar al finalizar las sesiones de trabajo.
- Los archivos que contengan información reservada, clasificada o datos personales deben ser almacenados en rutas que impidan el fácil acceso por terceros, no se deben almacenar en el área de escritorio de la pantalla del computador.
- El papel utilizado para imprimir información calificada como reservada o clasificada no debe ser utilizado para reciclar impresiones, la información

calificada como reservada o clasificada que ya no se utilice debe ser destruida de forma que no pueda ser reconstruida por personal no autorizado.

- Los funcionarios y contratistas responsables de la prestación de servicios para la UPIT que tengan dentro de sus responsabilidades la atención al público deberán almacenar los documentos y dispositivos de almacenamiento bajo llave y ubicar el equipo de cómputo de tal forma que se evite el acceso o revisión de la información por parte de los visitantes no autorizados.

4.7. Ubicación y seguridad de estaciones de trabajo

Las estaciones de trabajo deben estar en lugares en los que se reduzca el riesgo de daño por amenazas físicas como: fuego, agua, polvo, agentes químicos, vandalismo y sus pantallas se deben ubicar de forma que se reduzca la posibilidad de visualizar información calificada como reservada o clasificada por parte de personal no autorizado**.**

Las estaciones de trabajo de las instalaciones de la UPIT deben permanecer en oficinas que tengan controles de acceso físico y las estaciones designadas para actividades de teletrabajo deben permanecer supervisadas en todo momento o aseguradas físicamente para prevenir hurto o acceso a personal no autorizado.

Las líneas de suministro eléctrico de las estaciones de trabajo deben estas protegidas contra sobrevoltajes, corto circuito o descargas eléctricas por rayos.

4.8. Seguridad de los equipos fuera de las instalaciones

Para la seguridad de los equipos fuera de las instalaciones se deben cumplir los siguientes aspectos:

- Se deben mantener un registro de las personas que retiran equipos de la Entidad, bien sean funcionarios, contratistas o personal de mantenimiento y soporte.
- Se debe mantener registro de todos los equipos institucionales que salgan de las instalaciones de la UPIT.
- La Secretaría General puede definir el plazo máximo que se autoriza para la salida de computadores portátiles, tabletas y equipos de cómputo de la Entidad de acuerdo con las necesidades del servicio y naturaleza de la autorización de retiro.
- Con el fin de preservar la seguridad de los equipos de cómputo y medios de almacenamiento de propiedad de la UPIT que por razones de servicio o por

actividades de soporte y mantenimiento deban salir de las instalaciones de la Entidad, los autorizados para el retiro de equipos deben cumplir las siguientes políticas de seguridad:

a. La autorización para el retiro de equipos de cómputo o de almacenamiento de propiedad de la UPIT debe ser autorizada y remitida por el jefe de la persona a la Secretaría General.
b. Los equipos autorizados para salida permanente de los funcionarios de la UPIT deben ser registrados en la planilla de equipos con salida permanente que gestiona la mesa de ayuda de la UPIT.
c. Cuando se autorice el retiro temporal de equipos de propiedad de la UPIT se debe mantener un registro del tiempo que se autoriza la salida del equipo. La fecha de salida y la fecha en que el equipo volvió a las instalaciones de la Entidad
d. Los equipos propiedad de la Entidad no deben ser retirados sin seguros que cubran hurto o daño parcial o total.

Cuando los equipos de propiedad de la UPIT se retiren de las instalaciones, el responsable de su salida debe aplicar los siguientes controles de seguridad:

a. Nunca se deben dejar desatendidos los equipos cuando están fuera de las instalaciones de la Entidad, siempre deben estar a la vista o asegurados físicamente para prevenir su hurto.
b. Al salir de las instalaciones de la Entidad, los equipos deben ser transportados de tal forma que se eviten impactos que los puedan dañar, igualmente se debe prevenir que queden expuestos agentes ambientales como: sol directo, extremo calor, agua, tierra, agentes químicos que los puedan dañar.
c. En los casos en los que el equipo deba ser manipulado por múltiples personas, el responsable de la salida del equipo es la persona que debe mantener el control sobre que personas pueden utilizar el equipo fuera de las instalaciones de la UPIT.
d. Los equipos como computadores portátiles, tabletas o smartphones deben ser transportados como equipaje de mano bajo la custodia del responsable del equipo.
e. Informar al personal de vigilancia del edificio que se visita los detalles del computador que se ingresa, igualmente al salir del edificio visitado reportar el retiro del equipo

f. En lugares de trabajo expuestos a público los computadores portátiles deben permanecer aseguramos con guayas de seguridad a anclajes fijos o en su defecto nunca se deben desatender.
g. No se debe colocar el portátil sobre el piso o en lugares no visibles. Siempre se debe mantener a la vista.
h. No se deben escribir o pegar claves o contraseñas de portátiles o equipos en papeles o adhesivos a la cubierta o pantalla del equipo.
i. Únicamente el personal de mesa de ayuda o el personal debidamente autorizado para realizar actividades de soporte y mantenimiento puede hacer cambios en los equipos de la UPIT. Los responsables de retiro de equipo de la Entidad no deben hacer o permitir a personas no autorizadas realizar cambios físicos o lógicos sobre los equipos.
j. Los equipos o medios de almacenamiento de la UPIT autorizados para trabajar fuera de las instalaciones y que contengan información calificada como reservada o clasificada se deben cifrar mediante los procedimientos definidos por la mesa de ayuda antes de salir de la Entidad.
k. Toda la información que se gestione en computadores portátiles que salgan de la Entidad se debe almacenar en los repositorios compartidos de SharePoint institucional, en caso de robo o pérdida del equipo, la información almacenada en los repositorios institucionales se preserva.
l. Todos los equipos portátiles que se retiren de la Entidad deben mantener activo el protector de pantalla, el bloqueo de sesión con clave y la autenticación con clave. No se deben deshabilitar los controles de seguridad configurados por la mesa de ayuda en los equipos institucionales.
m. Por seguridad los equipos portátiles que salgan de las instalaciones deben tener bloqueados los puertos USB contra conexiones de medios de almacenamiento externo.
n. Por seguridad se debe evitar que personas no autorizadas utilicen los equipos de la Entidad cuando están fuera de las instalaciones.

4.9. Seguridad de medios de almacenamiento

El uso de periféricos y medios de almacenamiento externo (memorias USB, CD, cámaras, discos de almacenamiento externo, tarjetas de memoria y tablets), está permitido únicamente como medio tecnológico de apoyo al cumplimiento de las funciones asignadas a los servidores y partes interesadas responsables de la prestación de servicios de la UPIT, el uso de medios de almacenamiento institucionales extraíbles con fines personales está prohibido.

Según lo anterior, se debe considerar que:

- Todos Los medios de almacenamiento extraíbles deben permanecer bajo llave o en lugar seguro mientras no están en uso.
- Todo medio almacenamiento extraíble que contenga información calificada como reservada, clasificada o de carácter personal deber permanecer cifrado.
- Solo se deben usar medios extraíbles para almacenar información si es imposible usar los servicios de almacenamiento compartido SharePoint o One Drive gestionado por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.
- Todos los medios de almacenamiento extraíbles que se conecten a las estaciones de trabajo de la UPIT se deben verificar mediante el software antimalware para detectar y eliminar posibles amenazas.
- Se deben reportar a la mesa de ayuda la pérdida o hurto de medios de almacenamiento extraíbles de la UPIT que contengan información reservada, clasificada o de carácter personal.
- Las estaciones de trabajo asignadas para la administración de sistemas de información y componentes críticos de la infraestructura de comunicaciones y servicios de la UPIT deben tener deshabilitados por defecto los puertos USB para lectura de medios de almacenamiento extraíbles.
- Los medios de almacenamiento extraíbles no se deben usar como medios para almacenamiento de copias de respaldo, toda copia de respaldo se debe realizar en los repositorios compartido de SharePoint gestionados por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

4.10. Seguridad de servicios públicos esenciales

Los equipos de procesamiento y almacenamiento de información se deben mantener conectados a la red de energía regulada, para evitar deterioros por posibles fallas eléctricas.

Para proteger estos equipos de cortes eléctricos, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones debe mantener conectados los equipos críticos a un Sistema de Energía interrumpible como UPS y/o plantas eléctricas, para asegurar el apagado regulado y sistemático de los equipos de TIC, asegurando la continuidad de las operaciones mientras se restablece las fallas de suministro de energía eléctrica.

Los sistemas de refrigeración de los centros de datos deben permanecer siempre activos para prevenir daño a los equipos de comunicaciones, seguridad y procesamiento de datos de la UPIT.

Para evaluar el correcto funcionamiento de los servicios públicos esenciales del centro de datos, El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones realiza inspecciones semestrales con el apoyo de la compañía responsable del mantenimiento y gestión de estos servicios.

4.11. Seguridad del cableado

Respecto de la seguridad del cableado, se deben tener en cuenta los siguientes aspectos:

- El cableado de comunicaciones dentro de las instalaciones de la Entidad debe estar protegido para prevenir manipulación no autorizada.
- El cableado de comunicaciones debe estar separado de las redes eléctricas para prevenir interferencias electromagnéticas.
- Las redes de cableado eléctricas y de comunicaciones deben estar sujetas a mantenimiento periódico por parte de la empresa contratada por la UPIT.
- El cableado de comunicaciones y redes eléctricas dentro de las instalaciones de la UPIT debe estar claramente identificado para facilitar las tareas de mantenimiento y reparación.
- El acceso a los cuartos de equipos y cajas de conexión eléctrica y de comunicaciones debe estar restringido solamente al personal debidamente autorizado por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones debe verificar que se encuentren actualizados los planos o diagramas de ubicación física y de conectividad de los equipos de cómputo y semestralmente debe realizar pruebas de correcto funcionamiento del cableado y en caso de que se apliquen cambios que afecten al cableado se deberá realizar el proceso de certificación garantizando la calidad de sus componentes y su instalación.

4.12. Mantenimiento de equipos

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de verificar que los equipos de procesamiento y almacenamiento de información cuenten con contratos de soporte y

mantenimiento, de tal manera que es la encargada de coordinar las actividades de mantenimiento de los diferentes equipos de cómputo.

Los equipos deben contar con un plan de mantenimiento preventivo y correctivo que evite fallas en su funcionamiento y los resultados del mantenimiento deben ser registrados en informes que gestiona este Grupo Interno de Trabajo.

Cuando los proveedores de equipos de la UPIT deban realizar actividades de soporte o mantenimiento en las instalaciones de la UPIT, un colaborador de la Entidad debe supervisar las actividades del proveedor para prevenir acceso no autorizado a la información institucional. De esa forma, se debe considerar lo siguiente:

- Las actividades de soporte y mantenimiento remoto de equipos y servicios de la UPIT deben ser autorizadas por el personal del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones que es responsable de la administración de los equipos de tecnología de información y comunicaciones.
- Los mantenimientos de los servidores y servicios que soportan procesos misionales o de apoyo se deben gestionar a través del procedimiento de gestión de cambio del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.
- Cuando sea necesario dar de baja equipos debido a que no fue posible su reparación, se deben seguir los procedimientos de administración de bienes del sistema integrado de gestión institucional.

4.13. Disposición segura de equipos y medios de almacenamiento

En cuanto a la disposición segura de equipos y medios de almacenamiento, se tiene que:

- La información almacenada en activos de información, sistemas de información o medios físicos debe ser eliminada siguiendo los procedimientos legales, reglamentarios o contractuales cuando ya no es necesaria. La eliminación de información institucional debe seguir los lineamientos del proceso de gestión documental de la UPIT
- El periodo de retención de la información almacenada en activos de información, sistemas de información o medios físicos debe ser establecido por el programa institucional de gestión de archivo de la UPIT .
- Cuando se contrate a proveedores especializados en disposición final de información se debe requerir evidencia de la eliminación de la información.

- Cuando se contraten proveedores almacenamiento de información, se deben incluir cláusulas de eliminación definitiva de la información cuando finalice la prestación del servicio.
- Cuando se contraten servicios de nube se debe verificar la existencia de cláusulas en los contratos que contemplen la eliminación segura de la información al finalizar el contrato con el proveedor del servicio.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de determinar las técnicas apropiadas para realizar la eliminación segura de información reservada o confidencial de equipos de cómputo institucional m contemplando alternativas como:
    a. *Clearing*: Implica volver a escribir con un nuevo valor o usar una opción de menú del medio de almacenamiento para restablecer el dispositivo al estado de fábrica (donde no se admite la reescritura).
    b. Purga: se relaciona con técnicas físicas o lógicas que hacen que la recuperación de datos de destino sea inviable mediante técnicas de laboratorio de última generación.
    c. Destruir: hace que la recuperación de datos de destino sea inviable mediante técnicas de laboratorio de última generación y da como resultado la incapacidad posterior de usar los medios para el almacenamiento de datos.
- La destrucción de medios de almacenamiento considerados como obsoletos o en condición inservible debe realizarse siguiendo los lineamientos del programa de disposición final de residuos electrónicos de la UPIT.
- Cuando se utilicen servicios alquiler de equipos de cómputo, antes de la devolución del equipo al proveedor se deben aplicar técnicas de eliminación de los datos almacenados en la memoria y las unidades de disco de los equipos.

5. Controles tecnológicos

5.1. Seguridad de las estaciones de trabajo

Las estaciones de trabajo de la UPIT solo se deben utilizar para el cumplimiento de las labores y funciones designadas y está prohibido su uso para fines personales.

Para utilizar las estaciones de trabajo de la UPIT se deben atender los siguientes lineamientos:

- Se debe usar la cuenta de usuario y contraseña institucionales, la cual únicamente debe ser de conocimiento de la persona asignada y no debe ser compartir con ninguna persona.
- Se deben bloquear mientras no están en uso y las claves de acceso a las cuentas de usuario deben cumplir la Política de Contraseña Segura.
- El uso de puertos USB para conexión de dispositivos de almacenamiento debe permanecer bloqueado para estaciones de trabajo que gestionen información calificada como reservada, clasificada o datos personales.
- El uso de software de software de conexión remota para estaciones de trabajo con información reservada, clasificada y sensible personal debe permanecer bloqueado.
- El uso de periféricos (micrófonos, cámaras, lectores de huellas, scanner, impresoras) y medios de almacenamiento en las estaciones de trabajo se debe ser limitar de acuerdo con las funciones asignadas al colaborador de la UPIT.
- Las estaciones de trabajo y periféricos de la UPIT deben conectarse a la red eléctrica regulada para prevenir daños generados por fluctuaciones eléctricas y pérdida súbita de fluido eléctrico.
- Las estaciones de trabajo de la UPIT cuentan con una herramienta de protección contra software malicioso instalado y permanentemente actualizado, el software de protección contra códigos maliciosos siempre debe estar activo, actualizado y no se debe desactivar.
- Se debe verificar cualquier medio de almacenamiento externo que se requiera conectar a la estación de trabajo antes de usar los archivos y permitir que el software contra código malicioso elimine cualquier amenaza existente.
- La cuenta de usuario con privilegios de administración es de uso exclusivo del personal designado por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, los usuarios de las estaciones de trabajo no deben tener privilegios de administración sobre las estaciones de trabajo.
- Está prohibido realizar cambios en el hardware o software de las estaciones de trabajo de la UPIT, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia autorizada para autorizar y coordinar los cambios es las estaciones de trabajo.
- Está prohibido instalar software de cualquier naturaleza en las estaciones de trabajo de la UPIT, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia encargada de autorizar y coordinar la instalación, reconfiguración o actualización de software de las estaciones de trabajo.

5.2. Derechos de acceso privilegiado

La asignación de privilegios de acceso como administrador a los activos de información debe estar restringido solamente al personal del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones quienes actúan como administradores de servidores o estaciones de trabajo.

Las cuentas de usuario con privilegios de administrador a los activos de información solo se deben utilizar para labores de administración, nunca para tareas generales del día a día.

Cuando se asignen de privilegios de acceso como administrador a los activos de información se deben otorgar solo privilegios necesarios para realizar las labores asignadas.

Los roles o permisos como administrador de activos de información se deben suspender en caso de ausencia temporal o definitiva del responsable de la cuenta de usuario asignada y se deben revocar cuando se produzcan cambio de funciones o finalización a la vinculación laboral del responsable de la cuenta asignada.

Los roles o permisos temporales como administrador de activos de información asignados a proveedores de la UPIT para tareas de soporte y mantenimiento se deben revocar al finalizar las actividades.

El uso inapropiado de privilegios de acceso como administrador es un incidente de seguridad de la información, que se gestiona mediante el procedimiento de gestión de incidentes de seguridad de la información de la UPIT.

5.3. Restricción de acceso a la información

El acceso a la información, los sistemas de información y demás recursos informáticos de la UPIT se debe realizar con el usuario designado por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

El acceso a los activos de información de la UPIT se otorga aplicando las recomendaciones de estándares de seguridad reconocidos como NTC ISO 27001:2022 así:

a. Necesidad de uso: una persona, proceso o sistema informático solo tendrá acceso a la información que requiere para realizar las tareas que le han sido asignadas.
b. Mínimo privilegio: En general todo acceso está restringido a menos que sea explícitamente autorizado, solo se otorgan los permisos mínimos necesarios para realizar las tareas asignadas al colaborador de la UPIT.

Los responsables de procesos y dependencias son las personas encargadas de definir los permisos de acceso que se otorgan a los colaboradores de su área y son los únicos pueden solicitar el cambio o retiro de los controles de seguridad de acceso físico o acceso lógico de los activos de información que están bajo su responsabilidad.

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones configura los controles de acceso lógico a la información de acuerdo con los permisos aprobados por el responsable del proceso o dependencia.

El control de acceso a los activos de información almacenados en medios electrónicos se realiza mediante los controles de roles y privilegios configurados por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones. Los controles de acceso lógico contemplan el nivel de calificación de la información, los roles y funciones del personal al que se le otorgará el acceso.

Los responsables de proceso o dependencia pueden solicitar a la UPIT la protección de información calificada como reservada o clasificada que este bajo su responsabilidad con controles criptográficos. Las claves de acceso criptográfico de la información son gestionadas y custodiadas por la UPIT.

El acceso a áreas de almacenamiento de información en papel o medios físicos extraíbles está restringido solo al personal autorizado. Las áreas de almacenamiento de información física deben permanecer cerradas cuando no está presente personal de la UPIT y los controles de acceso físico (puertas, cerraduras, controles biométricos o sistemas de video vigilancia) no se deben deshabilitar en ningún momento, salvo por tareas de soporte o mantenimiento sobre esos equipos.

5.4. Acceso a código fuente de programas

El acceso al código fuente, librerías y demás componentes del software de la UPT está controlado y limitado únicamente al personal autorizado.

Las diferentes versiones del software se deben almacenar, controlar y proteger mediante herramientas que eviten cambios no controlados.

Por su parte, las bibliotecas y componentes de terceros que se utilicen para el desarrollo de software deben estar actualizadas, tener soporte y ser verificadas mediante pruebas de análisis de vulnerabilidades antes de su uso en ambientes de producción.

Las librerías y componentes de terceros deben obtenerse de fuentes comprobables y confiables y para ser utilizadas en los desarrollos de software de la UPIT deben contar con las licencias requeridas para su uso en el sistema de información final.

5.5. Autenticación Segura

Respecto de la autenticación segura se tiene que:

- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones asigna a cada funcionario o contratista de la UPIT una única cuenta de usuario para el acceso a los servicios tecnológicos de la Entidad.
- Cada cuenta de usuario de la UPIT se asigna a una única persona con el fin de poder responsabilizar a la persona de las acciones realizadas con la cuenta de usuario.
- Las cuentas de usuario para acceso a los activos de información, servicios tecnológicos y sistemas informáticos de la UPIT son personales e intransferibles.
- La asignación de cuentas de usuario compartidas que son gestionadas por varias personas solo se permite cuando por razones asociadas al cumplimiento de las funciones de la UPIT es indispensable contar con varios responsables de la cuenta. Toda cuenta de uso compartido debe ser autorizada por el jefe de la dependencia en donde se gestiona la cuenta compartida.
- La UPIT mantiene un registro de las cuentas de usuario y las personas responsables de las mismas.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones mantiene un registro de las cuentas de usuario que usan los servicios y procesos informáticos como pueden ser conexiones de bases de datos, servidores de páginas web, servicios de monitorización y en general cuentas que sean gestionadas por software sin intervención de personas.
- Las cuentas de usuario con privilegios de administrador tienen habilitado el registro de los eventos ejecutados con la cuenta de usuario.

- Para impedir uso no autorizado, suplantación de identidad y otros tipos de ataques informáticos, se deben mantener aseguradas las cuentas de usuario asignadas por terceras partes a la UPIT como, por ejemplo: redes sociales, servicios de información o sistemas de información de entidades de la rama ejecutiva (SECOP, Colombia Compra Eficiente y plataformas de administración de servicios como correo, servicios de nube, etc.).
- Las cuentas de usuario para acceso a servicios de ofimática (correo electrónico, almacenamiento SharePoint) se configuran con doble factor de autenticación.
- La UPIT lleva control y registro de los intentos de autenticación fallidos, para prevenir ataques informáticos las cuentas que superan tres (3) intentos de autenticación fallidos se deshabilitan hasta verificar las causas de la falla.
- Está prohibida la transmisión de claves de cuenta de usuario por canales inseguros. No se deben enviar contraseñas en texto claro.
- Las cuentas de usuario de conexión remota por VPN se desactivan después de treinta (30) minutos de inactividad.

5.5.1. Información de autenticación

La asignación de información para autenticación de las cuentas de usuario (contraseñas de usuario, configuración de doble factor de autenticación, tokens, etc.) se controla mediante el procedimiento de gestión de usuarios del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

Así las cosas, se debe tener en cuenta que:

- La información de autenticación como clave o contraseña para la cuenta de usuario es personal e intransferible.
- El uso de técnicas o herramientas para obtener sin autorización la información de autenticación de usuario es un incidente de seguridad de la información.
- Las claves o pines de acceso para autenticación de cualquier cuenta de usuario que sea afectada, comprometida o conocida por terceros no autorizados se deben cambiar a la mayor brevedad posible.
- La información biométrica para autenticación de cuenta de usuario, acceso a instalaciones físicas o acceso a activos de información debe protegerse de acuerdo con los lineamientos de la Ley Habeas Data.
- La utilización de contraseñas de usuario debe cumplir con la Política de Contraseña Segura.
- La información de autenticación para las cuentas de usuario asignadas a servicios informáticos como conexiones de bases de datos, servidores de páginas web, servicios de monitorización y en general cuentas de usuario que

son gestionadas por otros servicios de software solo debe ser conocida por el personal de administración servicios informáticos del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

- La seguridad de la información de autenticación de las cuentas de uso compartido autorizadas se debe proteger mediante software de gestión de contraseñas.
- La contraseña, clave, pin o pregunta de seguridad asignada a las cuentas de usuario proporcionados por terceros a la UPIT como: redes sociales, servicios de información o sistemas de información de entidades de la rama ejecutiva (SIFF, SECOP, Colombia Compra Eficiente, SIGEP, MUISCA, Ekogui, etc.), plataformas de administración de servicios como correo o servicios de nube, debe cambiarse cuando se utilice la cuenta por primera vez.
- Los responsables de la administración de las cuentas de usuario asignadas por terceros a la UPIT deben establecer los controles de protección de la información de autenticación incluyendo contraseñas de usuario seguras, configuración de doble factor de autenticación cuando aplique, cambio periódico de claves, impedir la reutilización de claves, entre otros controles que recomiende el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

5.6. Gestión de la capacidad

El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de orientar a todas las dependencias de la UPIT en la identificación de los requisitos de capacidad de procesamiento, almacenamiento y comunicaciones de la información para que garantice el cumplimiento de las obligaciones, objetivos y metas institucionales y en ese sentido, tiene las siguientes responsabilidades:

- Monitorizar los niveles de prestación de los servicios tecnológicos para tomar las medidas correctivas en caso de desviaciones que pongan en riesgo el cumplimiento de las obligaciones, objetivos y metas institucionales.
- Coordinar y supervisar la ejecución de pruebas que evalúen las capacidades de los recursos tecnológicos dispuestos para el procesamiento, almacenamiento y comunicaciones.
- Apoyar a todas las dependencias de la UPIT y liderar las actividades de identificación de oportunidades que mejoren la capacidad de los servicios tecnológicos: optimización del uso de almacenamiento, periodos de retención de copias de respaldo, optimización de sistemas de información, uso racional del ancho de banda, uso de servicios de computación en la nube, entre otros.

Los servicios de almacenamiento, procesamiento y comunicaciones pueden ser restringidos o suspendidos temporalmente por la UPIT en caso de identificar eventos o incidentes que pongan en riesgo la seguridad de la información institucional.

5.7. Protección contra códigos maliciosos

Respecto de la protección contra códigos maliciosos se tiene que:

- Todos los usuarios de la UPIT deben participar en las actividades de toma de conciencia en seguridad de la información para conocer las medidas de control y mecanismos de respuesta en caso de ataques por códigos maliciosos.
- Todas las estaciones de trabajo y los servidores de procesamiento de datos conectados a las redes de la UPIT se deben proteger con soluciones informáticas que prevengan ataques informáticos a través de códigos maliciosos.
- Todos los dispositivos informáticos conectados a la red de la UPIT y los recursos en red deberán tener un software contra códigos maliciosos instalado y configurado para que las firmas de detección estén actualizadas y se actualicen de forma rutinaria y automática.
- Las estaciones de trabajo y los servidores de procesamiento de datos, cuando sea factible, se deben configurar con reglas y controles que impidan el uso de software no autorizado.
- Los servidores de archivos conectados a la red local de la UPIT, debe utilizar el software de protección contra códigos maliciosos.
- Los servicios correo electrónico institucional deben utilizar el software de protección contra códigos maliciosos.
- En caso de contaminación por código maliciosos el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones puede coordinar la desconexión de equipos y servicios informáticos para prevenir la propagación de la amenaza. La contaminación por códigos maliciosos se gestiona mediante el procedimiento de gestión de incidentes de seguridad de la información.
- El software de protección contra códigos maliciosos no debe ser deshabilitado, todo cambio en la configuración del software contra códigos maliciosos debe ser autorizado por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.
- La frecuencia de actualización automática del software de protección contra códigos maliciosos no debe modificarse para reducir la frecuencia de las actualizaciones.

- Cualquier dispositivo de almacenamiento externo, archivo descargado desde correo o documento descargado de internet debe ser verificado por el software de protección contra códigos maliciosos antes de ser usado.
- Los servicios de acceso a Internet de la UPIT deben estar configurados con reglas o controles de acceso que eviten visitar sitios web maliciosos.
- Las estaciones de trabajo y trabajo y los servidores de procesamiento de datos deben ser sometidos a pruebas de análisis de vulnerabilidades antes de su entrada en producción y periódicamente durante su ciclo de vida.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de realizar seguimiento al cierre de vulnerabilidades detectadas en las estaciones de trabajo y los servidores de procesamiento de datos.
- El uso de uso de software códigos malicioso dentro de la red o en los activos de información de la UPIT, sus estaciones de trabajo, servidores de procesamiento de datos, servicios informáticos, plataforma de almacenamiento y en general sobre su infraestructura tecnológica institucional es un delito informático que se gestiona a través del procedimiento de gestión de incidentes de seguridad de la información.[1]

5.8. Gestión de Vulnerabilidades técnicas

Con relación a la gestión de vulnerabilidades técnicas, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de:

- Coordinar las actividades de recopilación de información sobre vulnerabilidades técnicas en fuentes oficiales sobre amenazas informáticas con: proveedores reconocidos de soluciones de seguridad de la información y ciberseguridad y en grupos de interés especializados en seguridad informática.
- Coordinar las actividades de evaluación de seguridad de software de código abierto, bibliotecas de terceros, *framework* de desarrollo y componentes de terceros que se utilicen en los desarrollos de software de la UPIT.
- Liderar la actualización de riesgos de seguridad de la información, ciberseguridad y protección de datos personales cuando se detecten vulnerabilidades técnicas sobre los activos de información institucionales.

[1] 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. Art 269e

- Coordinar las pruebas de análisis y detección de vulnerabilidades y las pruebas de penetración sobre la infraestructura tecnológica de la UPIT.
- Realizar seguimiento al cierre de vulnerabilidades detectadas en las estaciones de trabajo y los servidores de procesamiento de datos.

Así las cosas, Todos los funcionarios de la UPIT y partes interesadas responsables de la prestación de servicios para la UPIT deben informar a El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones cualquier vulnerabilidad que detecten en los activos de información.

Las estaciones de trabajo y los servidores de procesamiento de datos deben ser sometidos a pruebas de análisis de vulnerabilidades antes de su entrada en producción y periódicamente durante su ciclo de vida.

Los activos de información, servicios informáticos, sistemas de información y los servidores de procesamiento de datos se debe someter a pruebas de penetración controladas (hacking ético) por parte de personal competente para identificar vulnerabilidades y determinar si su explotación es exitosa.

Los contratos con proveedores de servicios y las terceras partes responsables de prestación de servicios informáticos deben incluir cláusulas sobre notificación, manejo y resolución de vulnerabilidades de los servicios contratados para la UPIT.

5.9. Gestión de configuración de seguridad

- Todos los dispositivos, servicios y componentes de la infraestructura de tecnología de información y comunicaciones de la UPIT deben contar una descripción de la línea base de seguridad recomendada para una operación seguridad del activo de información.[2]
- Las líneas base de seguridad se deben definir tomando en cuenta las recomendaciones de seguridad de los fabricantes de equipos, proveedores de los servicios de la UPIT y estándares de seguridad de la información como CIS (Center for Internet Security).
- La línea base de seguridad debe actualizarse como resultado de las actualizaciones de seguridad formuladas por los fabricantes y proveedores de servicios de la Entidad.

[2] Ver https://workbench.cisecurity.org/files

- La línea base de seguridad debe actualizarse de acuerdo con los resultados de las pruebas de análisis de vulnerabilidades y ethical hacking que se realicen al dispositivo, servicio o componente de infraestructura tecnológica
- El cumplimiento de la línea base de seguridad se debe verificar antes de que el dispositivo, servicio o componente de infraestructura tecnológica sea puesto en producción o sometido a cambios autorizados.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de mantener y coordinar la actualización de la documentación de línea de base de seguridad que deben cumplir los dispositivos, servicio o componente de infraestructura tecnológica institucional.

5.10. Eliminación de información

La eliminación de información institucional que ha perdido valor institucional o ya no es necesaria para el cumplimiento de requisitos legales o normativos se puede eliminar de sistemas de información, medios de almacenamiento extraíbles o medios físicos como papel siguiendo los lineamientos del proceso de gestión documental y archivo.

La información calificada como reservada o clasificada no se debe almacenar más allá del tiempo exigido por los requisitos legales o normativos para prevenir divulgación innecesaria.

En todo caso, se debe considerar que:

- Cuando se contrate los servicios de custodia de información institucional con terceros se debe considerar la aplicación de cláusulas de eliminación segura de copias de la información cuando finalice la relación contractual con el proveedor.
- La eliminación segura de información almacenada en dispositivos electrónicos debe seguir los lineamientos de la Política Disposición segura de equipos y medios de almacenamiento.
- Cuando se contraten servicios de almacenamiento de información en la nube, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones debe validar con el proveedor del servicio, que el mecanismo de eliminación segura de la información que se aplique garantiza el borrado seguro de los datos.
- Cuando se utilicen servicios de arrendamiento de estacione de trabajo, se debe garantizar que antes de devolver el equipo al proveedor se realice un borrado

seguro de cualquier dato institucional que haya sido almacenado en el equipo arrendado.

- Cuando se requiera realizar la eliminación segura de información almacenada en teléfonos móviles institucionales se deben considerar el restablecimiento del equipo a configuración inicial de fabrica o su destrucción aplicando la política institucional de manejo de residuos electrónicos

5.11. Enmascaramiento (anonimización) de Información

Los datos personales calificados como como sensibles, privados o semiprivados[3] deben ser sometidos a procesos de anonimización[4] cuando se ordene su publicación por mandato legal.

La aplicación de procesos de anonimización de datos personales se debe realizar para delimitar y suprimir toda aquella información que permita identificar a una persona, con el objetivo eliminar de forma irreversible y permanente cualquier posibilidad de identificación de dicho individuo y poder compartir los datos anónimos para fines estadísticos o de investigación.

En ese sentido, se debe atender lo siguiente:

- La información calificada como reservada, clasificada o personal almacenado en medios de almacenamiento extraíbles deben ser cifrada de acuerdo con la política de cifrado de datos de la UPIT.
- Las transmisiones de información calificada como reservada, clasificada o personal deben ser cifradas de acuerdo con la política de cifrado de datos.
- Las descargas masivas de datos desde repositorios de información de la UPIT deben ser supervisadas para prevenir fuga de datos.

[3] 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

[4] Anonimización: Es el proceso mediante el cual se condiciona un conjunto de datos de modo que no se pueda identificar a una persona, pero pueda ser utilizada para realizar análisis técnico y científico válido sobre ese conjunto de datos (Guía de Anonimización de Datos Estructurados del Archivo General de la Nación) / Anonimización: Proceso por el cual la información de identificación personal se modifica de forma irreversible de tal manera que no se pueda identificar, directa o indirectamente, ya sea por sus propios medios o en colaboración con algún tercero, a la persona asociada a dicha información de identificación personal. (Estándar ISO / IEC 29100:2011, 2011).

- El tamaño de los adjuntos en los servicios de correo electrónico debe limitarse para prevenir transmisión masiva de datos. El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones en coordinación con las dependencias de la UPIT es responsable de establecer el tamaño máximo de adjuntos para los servicios de correo electrónico institucional.
- Se debe restringir la instalación y uso de software para transmisión de archivos únicamente al personal autorizado el responsable del proceso.
- Las conexiones de las estaciones de trabajo a las redes de la UPIT deben estar controladas por el controlador de Dominio y limitar el acceso solo a los servicios necesarios para el cumplimiento de las labores asignadas funcionario o parte interesada responsable de la prestación de servicios para la UPIT.
- Los servicios de almacenamiento de datos en nube deben habilitar los controles disponibles de prevención de fuga de datos.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones debe restringir el uso de plataformas de almacenamiento de nube, únicamente a los servicios oficialmente contratados por la Entidad.
- Los usuarios de servicios de impresión deben retirar las impresiones de información reservada, clasificado o personal una finaliza el trabajo de impresión.

5.12. Prevención de Fuga de Datos

Para la prevención de fuga de datos, se debe tener en cuenta que:

- Todo el personal que presta sus servicios para la UPIT debe participar en las actividades de capacitación y sensibilización en seguridad de la información y prevención de fuga de datos.
- La información calificada como reservada, clasificada o personal debe estar claramente identificada para prevenir su divulgación no autorizada o fuga.
- El acceso a información calificada como reservada, clasificada o personal debe estar restringido únicamente al personal que por la naturaleza de sus funciones deben realizar tratamiento de esa información.
- La información calificada como reservada, clasificada o personal almacenado en medios de almacenamiento extraíbles deben ser cifrada de acuerdo con la política de cifrado de datos de la UPIT .
- Las transmisiones de información calificada como reservada, clasificada o personal deben ser cifradas de acuerdo con la política de cifrado de datos.
- Las descargas masivas de datos desde repositorios de información de la UPIT deben ser supervisadas para prevenir fuga de datos.

- El tamaño de los adjuntos en los servicios de correo electrónico debe limitarse para prevenir transmisión masiva de datos. La Oficina de Gestión de la Información en coordinación con las dependencias de la UPIT es responsable de establecer el tamaño máximo de adjuntos para los servicios de correo electrónico institucional.
- Se debe restringir la instalación y uso de software para transmisión de archivos únicamente al personal autorizado el responsable del proceso.
- Las conexiones de las estaciones de trabajo a las redes de la UPIT deben estar controladas por el controlador de Dominio y limitar el acceso solo a los servicios necesarios para el cumplimiento de las labores asignadas funcionario o parte interesada responsable de la prestación de servicios para la UPIT.
- Los servicios de almacenamiento de datos en nube deben habilitar los controles disponibles de prevención de fuga de datos.
- La Oficina de Gestión de la Información debe restringir el uso de plataformas de almacenamiento de nube, únicamente a los servicios oficialmente contratados por la Entidad.
- Los usuarios de servicios de impresión deben retirar las impresiones de información reservada, clasificado o personal una finaliza el trabajo de impresión.

5.13. Copias de seguridad

La información requerida para el cumplimiento de las actividades institucionales de la UPIT debe ser respaldada a intervalos planificados, la frecuencia, forma y periodo de retención de las copias de respaldo debe permitir el cumplimiento de los requisitos legales, requisitos de las tablas de retención documental, los niveles de clasificación de la información, los planes de tratamiento de riesgos, la estrategia de recuperación ante desastres y las capacidades tecnológicas de las UPIT.

Con el apoyo del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, los responsables de procesos o jefes de dependencia establecen la información que debe ser respaldada, la periodicidad de la copia de respaldo y los tiempos de preservación de las copias de respaldo.

De esa forma, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones tiene las siguientes responsabilidades:

- Definir los mecanismos tecnológicos para la ejecución y preservación de las copias de respaldo garantizando su confidencialidad, integridad y disponibilidad.

- Realizar verificación del correcto funcionamiento de las copias de respaldo mediante pruebas de restauración.
- Mantener registro de la ejecución de copias de respaldo y restauración.

Los responsables de procesos o coordinadores de dependencias pueden solicitar la ejecución las pruebas de las copias de respaldo al Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones para verificar su correcto funcionamiento.

Con el fin de prevenir la perdida de información cuando se utilizan servicios de nube, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones puede coordinar la ejecución de copias de respaldo de la información en medios externos o nubes separadas a la definida para los procesos normales de producción institucional.

5.14. Redundancia de instalaciones de procesamiento

- Mediante el diseño y planificación de un plan de recuperación ante desastres El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones establece la arquitectura tecnológica necesaria para garantizar la prestación de servicios tecnológicos institucionales en caso de contingencias de orden mayor.
- Los sistemas de información críticos de la UPIT y los dispositivos que los soportan deben contar con redundancias que permitan la continuidad de los servicios institucionales en caso de materialización de eventos de desastre.
- Anualmente el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones debe realizar pruebas del correcto funcionamiento Los sistemas redundantes deben ser sometidos a pruebas anualmente para comprobar su correcto funcionamiento.
- La verificación del correcto funcionamiento de los planes de recuperación ante desastres debe incluir pruebas de restauración de la información críticas de la UPIT.
- Con el fin de prevenir las pérdidas de conexión a los servicios institucionales de procesamiento y almacenamiento en nube, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones puede establecer la necesidad de contar con canales de comunicación redundantes para el servicio de acceso a Internet.

5.15. Registro de eventos

Los sistemas de información, dispositivos de procesamiento y comunicaciones de la UPIT deben ser configurados para que registren actividades excepcionales, fallas y otros eventos destacados que permitan diagnosticar problemas o incidentes de seguridad de la información.

Los registros de eventos de los sistemas de información, dispositivos de procesamiento y comunicaciones deben incluir mínimo: fecha y hora, detalles descriptivos del evento, identificación del dispositivo que detectar el evento, o del dispositivo que generó el registro de evento.
Se deben considerar como actividades excepcionales entre otros:

- Intentos fallidos de autenticación.
- Acceso exitoso a recursos de almacenamiento o servicios tecnológicos.
- Cambios en los archivos de configuración de servicios tecnológicos.
- Conexiones con usuarios que tiene privilegios de administración.
- Alarmas de sistemas de control de acceso.
- Alertas del software antimalware.
- Alertas de los sistemas de protección perimetral: firewall.
- Creación, eliminación y modificación de cuentas y perfiles de usuario.

Los registros de eventos se deben preservar de acuerdo con la política de Protección de registros.

5.16. Monitorización de eventos

Los eventos reportados por los dispositivos de procesamiento, almacenamiento y comunicaciones e la infraestructura TIC de la UPIT deben verificados cuando se registren actividades excepcionales.

Los administradores de servicios y equipos tecnológicos de la UPIT deben evaluar los registros de eventos y determinar las medidas necesarias para su tratamiento de acuerdo con la naturaleza de este.

Los eventos, registros y alertas de los dispositivos TIC deben ser monitorizadas por el personal del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones que administra los servicios tecnológicos institucionales.

Cuando se identifique eventos que sean indicios de posibles incidentes de seguridad de la información se debe realizar su reporte al responsable de seguridad de la información para su evaluación.

Los registros de eventos de seguridad se deben proteger de acuerdo con la política de Protección de Registros.

Dentro de los eventos que deben ser monitorizados periódicamente se debe contemplar:

- Tráfico entrante y saliente de las redes de datos de la UPIT
- Acceso a servidores, sistemas de información, equipos de seguridad y comunicaciones
- Registros de dispositivos de seguridad: antimalware, firewall, proxy
- Uso de recursos de los servidores: CPU, almacenamiento, memoria, ancho de banda, rendimiento general del equipo.
- Patrones de comportamiento típicos de ataques informáticos: escaneo de puertos, denegación de servicios, modificaciones en portales, saturación de consultas en DNS, tráfico anómalo de fuentes identificadas por COLCERT, CSIRT y otros organismos especializados en seguridad informática.

Los administradores de infraestructura tecnológica de la UPIT deben mantener una línea base de desempeño normal de las plataformas para identificar patrones excepcionales.

5.17. Sincronización de relojes

La hora de los sistemas de información, dispositivos de comunicaciones, dispositivos de seguridad, estaciones de trabajo y en general cualquier dispositivo electrónico con capacidad de generar registro de eventos debe estar sincronizada con la hora legal colombiana establecida por el Instituto Nacional de Metrología. https://horalegal.inm.gov.co/

Los registros de auditoría de bases de datos, sistemas de información y demás de registros de eventos sobre sistemas de información o servicios informáticos deben estar sincronizados con la hora legal colombiana establecida por el Instituto Nacional de Metrología.

5.18. Uso de programas utilitarios

Los usuarios de equipos y servicios tecnológicos de la UPIT no deben instalar programas que puedan anular los controles de seguridad de las estaciones de trabajo o de las aplicaciones. Solamente los administradores de servicios y plataformas de la UPIT tienen autorización del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones para el uso de software y utilidades especiales para gestión de servicios tecnológicos.

La instalación y uso de programas utilitarios debe ser restringida a las cuentas de administración de equipos, las cuales son responsabilidad de personal del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones. Los diferentes equipos tecnológicos de la UPIT deben mantener restringido el acceso a cuentas de administración o puertos de acceso con nivel de administrador.

5.19. Instalación de software en sistemas operacionales

- La instalación de software en los sistemas operacionales de las estaciones de trabajo y servidores de la UPIT solo debe ser realizada por el personal autorizado por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.
- La instalación de actualizaciones y parches de seguridad en estaciones de trabajo y servidores solo debe ser realizada por los administradores de los equipos o el personal autorizado por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.
- La instalación de nuevo software o cambios en el software de los servidores de la UPIT está controlada para prevenir pérdidas de disponibilidad de los servicios tecnológicos, todo cambio se debe realizar aplicando el procedimiento de gestión de cambios del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.
- Los administradores de servicios y servidores de la UPIT deben verificar la existencia de copias de respaldo de la configuración y datos de los servidores antes de realizar cambios en los servidores de la Entidad
- Al finalizar la instalación de nuevo software o aplicación de cambios en el software de los servidores se deben realizar pruebas de análisis de vulnerabilidades para identificar brechas de seguridad.
- Al finalizar la instalación de nuevo software o aplicación de cambios en el software se debe realizar aseguramiento (*hardenning*) de los servidores y cierre de las vulnerabilidades identificadas antes de su paso a producción.

- La instalación automática de parches de seguridad o actualizaciones en el software debe estar contralada y solo se debe realizar de fuentes oficiales del proveedor del sistema operacional o el software.
- El sistema operacional y software de los servidores deben mantenerse en las versiones soportadas por los contratos suscritos por la UPIT.
- La actualización de sistemas operacionales, parches, software, librerías o módulos deben mantener la compatibilidad con los demás componentes de sistema de información modificado.
- El software de código abierto, librerías, módulos o *framework* de desarrollo debe mantenerse en versiones compatibles, estables y soportadas por los sistemas de información que los utilizan.
- Los derechos de acceso privilegiado asignados a proveedores o terceras partes responsables de prestación solo se deben asignar al momento de realizar las instalaciones o cambios y se deben retirar cuando se completa exitosamente o se cancela el cambio en el sistema operacional o el software.
- Cualquier cambio de configuración en el sistema operacional de servidores de la UPIT debe contar con una estrategia de reversión en caso de fallas.
- Cuando se permita realizar cambios en los equipos o servicios de la Entidad a los proveedores , se deben monitorizar los cambios realizados.

5.20. Seguridad de las redes

5.20.1. Redes VPN

- Las conexiones VPN (red privada virtual) hacia la red local de la UPIT deben ser solicitadas por los responsables de proceso o el jefe de la dependencia a través de la mesa de ayuda de la UPIT.
- Las conexiones remotas a estaciones de trabajo de la UPIT deben ser solicitadas por los responsables de los procesos o jefes de dependencia.
- Las conexiones remotas por redes privadas virtuales a las redes local de la UPIT o a sus estaciones de trabajo son evaluadas para aprobación por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones de acuerdo con la disponibilidad de canales de acceso y potenciales riesgos de seguridad que se identifiquen sobre el acceso solicitado.
- Las contraseñas de uso de las redes privadas virtuales deben cumplir la política de contraseñas seguras.
- La conexión desde redes privadas virtuales con capacidades para uso de doble factor de autenticación, deben ser configuradas para aplicar esos controles de múltiple factor de autenticación.

- Las redes privadas virtuales deben utilizar algoritmos de cifrados seguros, como mínimo recomendado el SHA-256 con AES 128/256 o SHA-384, en caso de información muy sensible.
- La conexión por VPN a la red local de la UPIT se debe realizar únicamente con el software autorizado por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de definir la modalidad de conexión de las redes privadas virtuales: sitio a sitio (site-to-site), cliente a servidor(client-to-site).
- El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones mantiene un registro de las conexiones VPN realizadas por el personal de la UPIT con el objetivo de evaluar calidad de servicio y monitorizar eventos de seguridad. Los datos transmitidos a través de la VPN están protegidos con técnicas criptográficas que previenen la pérdida de confidencialidad.
- La descarga de datos a través de redes privadas virtuales se monitoriza y limita para prevenir fuga de datos.
- Las conexiones por VPN deben se configuradas para un periodo máximo de conexión, tiempo después del cual se debe reiniciar la conexión si el usuario lo requiere.
- Las conexiones por red privada virtual deben ser registradas en una bitácora que incluya usuario autorizado, servicios o servidores a los que se autoriza el acceso, fecha de expiración del acceso.
- Las conexiones por red privada virtual deben ser configuradas con usuarios sin privilegios de administración.
- Los servidores de redes privadas virtuales se someten a pruebas de análisis de vulnerabilidades, se aseguran para cerrar vulnerabilidades y se actualizan con los parches de seguridad recomendados para cerrar brechas de seguridad.

5.20.2. Seguridad de redes inalámbricas

- Las conexiones a las redes Wifi de la UPIT se configuran con clave de control de acceso para prevenir accesos no autorizados
- Los SSID (identificadores de nombre de red) de las redes Wifi de la UPIT debe seguir el estándar de nombre definido por El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, no se deben usar los nombres predeterminados definidos por los fabricantes.
- Los dispositivos de acceso a redes inalámbrica deben tener desactivada la difusión del identificador de red SSID (*Service Set Identifier*) para evitar que el dispositivo inalámbrico anuncie su presencia a personas no autorizadas.

- Las claves de administración de los dispositivos de acceso a redes inalámbrica deben cumplir con la política de contraseña segura de la UPIT.
- Las contraseñas de acceso a las redes Wifi de la UPIT deben cumplir con la política de contraseña segura de la UPIT.
- Toda conexión a red Wifi de la UPIT debe ser configurada con protocolo seguro de autenticación, mínimo WPA2.
- Las configuraciones de conexión de las redes inalámbricas se deben configurarse para cifrar por defecto todo el tráfico, mínimo con protocolo AES.
- El firmware de los dispositivos de acceso a redes inalámbricas debe estar siempre actualizado al último parche de seguridad recomendado por el fabricante. Se debe preferir la actualización automática de parches de seguridad.
- Los accesos de red inalámbrica para invitados a las instalaciones de la UPIT deben ser configurados en segmentos de red separados a las redes de producción.
- El acceso de red inalámbrica para invitados a las instalaciones de la UPIT se debe limitar en el tiempo y aun número máximo diario de conexiones por invitado.
- La configuración de rango de direcciones IP que puede otorgar el dispositivo de acceso a redes inalámbricas (Access Point) se debe limitar al número mínimo necesario para prestar con oportunidad y efectividad el servicio a los servidores, visitantes y proveedores responsables de la prestación de servicios para la UPIT.
- Los dispositivos de acceso a redes inalámbricas (Access Point) se deben configurar para limitar la potencia de radiación de su señal al mínimo necesario para prestar el servicio de manera efectiva y segura.
- Los dispositivos de acceso a redes inalámbrica deben tener deshabilitada la opción de configuración remota.
- En los dispositivos de acceso a redes inalámbricas se debe deshabilitar el protocolo UPnP (*Universal Plug and Play*)
- Los dispositivos de acceso a redes inalámbricas deben ser sometidos mínimo una vez al año a pruebas de análisis de vulnerabilidades y *ethical hacking*.
- Los corta fuegos de los dispositivos de acceso a redes inalámbricas deben habilitarse y configurarse para prevenir accesos no autorizados.

5.21. Segregación de redes

Las redes de datos alambradas o inalámbricas están segmentadas para lograr un control efectivo del tráfico al interior de las redes de la UPIT, los administradores de los servicios de red aplican políticas de segmentación de tráfico sobre la diferentes redes y subredes de la infraestructura de comunicaciones de la UPIT para mitigar riesgos de pérdida de confidencialidad de la información.

Las configuraciones de seguridad de las diferentes redes y subredes se diseñan aplicando principios de Zero Trust lo que significa que no se puede considerar por defecto como seguro ningún tipo de tráfico externo o interno dentro de las redes de la UPIT.

Los siguientes activos de información deben evaluar la aplicación de configuraciones de segmentación de tráfico de red para prevenir acceso no autorizado a la información de la Entidad:

- Redes inalámbricas para uso de invitados o personal no vinculado a la Entidad
- Servicios de nube Pública
- Grupos de usuarios por dependencias
- La segmentación de las diferentes redes puede realizarse mediante configuraciones físicas a través de dispositivos tipo firewall o mediante Redes locales virtuales VLAN

En los casos en que el nivel de sensibilidad de la información gestionada por los diferentes grupos de usuarios demande mayores niveles de seguridad El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones puede contemplar la aplicación de configuraciones de microsegmentación de las redes de acuerdo con las capacidades de los dispositivos de comunicaciones.

5.22. Filtrado WEB

Con el objetivo de prevenir el acceso no autorizado a sitios de Internet potencialmente peligrosos El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones configura los firewalls institucionales para evitar la navegación en sitios web con contenidos marcado como:

- Contenido para adultos.
- Juegos en línea.
- Contenido sexual explícito.
- Acceso a código malicioso.
- Ventas on line.
- Servicios de descarga masivo de contenidos: servicios de video streamming, redes p2p, descarga de material multimedia.
- Terrorismo

5.23. Uso de criptografía

- La UPIT aplica controles criptográficos sobre sus redes inalámbricas y conexiones VPN para prevenir pérdida de confidencialidad de la información institucional
- El tráfico de redes inalámbricas se protege mediante cifrado WPA2. Ver política de Seguridad de redes inalámbrica.
- El acceso seguro a servidores se debe realizar con protocolos que garanticen cifrado de los datos, se debe usar protocolo de conexión SSH, SFTP/FTPS, HTTPS.
- El tráfico de los sitios web de la UPIT debe estar protegido mediante certificados seguros emitidos por entidades de certificación avaladas. Los certificados para sitios web deben cumplir estándares internacionales como TLS v1.2 o TLS v 1.3 o superior.
- Los certificados y firmas digitales utilizados para los documentos y servicios de información la Entidad deben ser generados por entidades de certificación avaladas por la Superintendencia de Industria y Comercio.
- Las claves criptográficas utilizadas para cifrar la información deben cumplir con la política de contraseña segura o superior.
- Cuando la UPIT requiera la aplicación de cifrado de datos en medios de almacenamiento, el estándar debe ser igual o superior al estándar Cifrado AES-256 *Advanced Encryption Standard* (AES).
- La UPIT aplica controles criptográficos a la información calificada como reservada, clasificada y a los datos personales sensibles cuando se transmitan por redes de datos que no garanticen la seguridad de los datos.
- Se aplican controles criptográficos a la información calificada como reservada, clasificada y a los datos personales sensibles almacenada en medios de almacenamiento extraíbles o computadores portátiles autorizados para salir de las instalaciones de la UPIT
- La UPIT aplica controles criptográficos a la información de carácter personal que se transfiere a terceras partes con ocasión de mandato legal o acuerdos establecidos por la UPIT.
- Las claves de los diferentes servicios de cifrado de datos son gestionadas por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones

5.24. Ciclo de Vida de desarrollo Seguro

Para el desarrollo de software la UPIT se realiza el análisis del requerimiento que origina el desarrollo, en donde se determina metodología a utilizar (P.e. Metodología

ágil, *Rapid application development, Scrum, Extreme Programming*,), las etapas de desarrollo, la estructura de desglose de trabajo, los responsables, criterios de aceptación, las pruebas de funcionalidad, seguridad y pruebas integrales; que den cuenta del cumplimiento de los requerimientos y el cumplimiento de los objetivos estratégicos de la UPIT.

La identificación de las necesidades y requisitos de funcionalidad, calidad y seguridad se realiza en coordinación entre el área solicitante y El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

Para el desarrollo y puesta de producción del software, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones dispone tener presente tres ambientes separados así: i) de desarrollo (puede ser en los equipos asignados a los colaboradores), ii) de pruebas y iii) de producción, evitando así las alteraciones o modificaciones no autorizadas del código fuente.

5.25. Identificación y documentación de requisitos de seguridad de la información

Los desarrollos de software o sistemas de información de la UPIT siempre consideran actividades para identificar:

a. Requisitos de seguridad de la información, ciberseguridad y protección de datos personales.
b. Los requisitos de acceso a la información y los roles que participarán para el tratamiento de la información.
c. Identificación, valoración, evaluación y tratamiento de riesgos de seguridad de la información, ciberseguridad y protección de datos personales que pueden afectar el procesamiento de los datos en el sistema de información.

Los desarrollos de software y sistemas de información deben ser diseñados con protección de privacidad de datos personales por defecto y debe contemplar:

a. Necesidades de segregación de funciones y niveles de acceso a la información que procesará el sistema.
b. Requisitos de resiliencia contra ataques informáticos o interrupciones no intensionales.
c. Protección de la información cuando los datos están en su fase de procesamiento, almacenamiento o tránsito.

d. Aspectos de cifrado de la información en su almacenamiento o tránsito y tiempos de conservación.
e. Necesidades de auditoría y registro de eventos de las actividades realizadas en el sistema de información.

5.26. Arquitectura segura de sistemas y principios de ingeniería

La Arquitectura de los sistemas de información y soluciones de software para la UPIT deben considerar los requisitos de seguridad de la información en todas las capas del sistema, incluidas, pero sin limitarse a: requisitos de negocio, modelo de datos, requisitos de aplicación, tecnología. Esta arquitectura debe considerar la aplicación de principios de arquitectura segura del software, incluidos, pero sin limitarse a:

- Seguridad en el diseño: La seguridad se debe soportar en controles específicos y probados en lugar de "seguridad por oscuridad"
- Defensa en profundidad: La seguridad se debe implementar en varias capas de defensa
- Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que la seguridad siempre este presente.
- Denegación predeterminada: Los sistemas se deben diseñar considerando que los usuarios inicialmente no tendrán ninguna función habilitada y solo se les habilitará las funciones necesarias para el desarrollo de sus tareas.
- Zero Trust: Los sistemas se deben diseñar considerando que no existe una barrera absoluta entre lo que es confiable y lo que no es confiable en una red y que, por lo tanto, todo debe ser verificado.
- Fallo seguro: El sistema se debe diseñar para que, en caso de falla, pase a un estado seguro de protección de datos y recursos.
- Desconfianza de entradas externas: Todas las entradas externas al sistema se deben considerar inseguras y se deben verificar antes de su uso.
- Seguridad en la implementación: La implementación del sistema se debe realizar asumiendo que estarán expuestos a ambiente inseguro y hostil.
- Privilegio Mínimo: Solo se deben otorgar los permisos necesarios para realizar las tareas asignadas.
- Usabilidad y Manejabilidad: Los controles de seguridad deben ser transparentes para el usuario y no deben causar esfuerzos adicionales innecesarios para el uso del sistema.
- Funcionalidad mínima: El acceso a las funcionalidades del sistema se debe realizar con mínimos privilegios.

5.27. Principios de construcción y codificación segura de los sistemas

El software que se desarrolle para los sistemas de información o servicios de la UPIT debe seguir lineamientos de codificación segura para que se reduzca la probabilidad de introducir vulnerabilidades en los servicios.

Los equipos que desarrollen sistemas de información, componentes o librerías para la UPIT deben aplicar buenas prácticas de codificación segura y adoptar principios como:

- Seguridad por diseño: La seguridad en la codificación debe estar presente desde el diseño del sistema o componente. Desde las primeras etapas de codificación se deben aplicar controles de validación de campos de entrada, control de acceso, gestión de contraseñas, manejo de errores y excepciones, cifrado de datos entre otros controles.
- Denegación por defecto: Por defecto todo acceso debe ser negado y el modelo de permisos es el que debe determinar cuáles accesos a datos o funcionalidades se autorizan.
- Principio de mínimo privilegio: Cada proceso debe ejecutarse con el menor conjunto de privilegios necesarios para completar el trabajo. Solo se debe acceder a cualquier permiso privilegiado durante el menor tiempo necesario para completar la tarea.
- Minimización y ofuscación de código: El código debe ser claro y limpio, el uso de codificación compleja buscando que sea de difícil lectura para posibles atacantes se debe evitar porque hace difícil el mantenimiento del código.
- Evitar atajos: No se debe pasar por alto la aplicación de controles de seguridad en el código fuente para intentar acelerar el paso a producción del software.
- Evitar resolver las vulnerabilidades al final del desarrollo: Las vulnerabilidades identificadas durante la etapa de codificación se deben resolver lo antes posible para evitar propagación de brechas de seguridad a lo largo de todo el sistema
- Escaneo automatizado y revisiones de código: El código fuente debería ser verificado con herramientas de revisión de código fuente. El código ejecutable debe ser sometido a pruebas automatizadas de análisis de vulnerabilidades para identificar brechas de seguridad.
- Evitar componentes con vulnerabilidades conocidas: Aunque los componentes y bibliotecas de código abierto, a menudo consumidos como paquetes, pueden ahorrar tiempo y energía a los desarrolladores, también son un punto de entrada para atacantes y fuente de vulnerabilidades.
- Auditoria y Registro: El software que cuenta con registros de auditoria permite detectar posibles incidentes en su entorno de producción.

5.28. Software de código abierto

- El uso de software de código abierto para el desarrollo de sistemas de información y soluciones de software de la UPIT se debe realizar a partir de fuentes obtenidas legalmente con la autorización de su autor expresada según el modo y vigencia de licenciamiento.
- Todo software de código abierto incluidas las herramientas de desarrollo, framework, librerías y componentes debe someterse a pruebas de seguridad, análisis de vulnerabilidades y *ethical hacking* durante la fase de pruebas del sistema de información o solución de software.
- El registro de los sistemas de información y soluciones de software de la UPIT que haga uso de módulos, componentes o librerías de código abierto debe cumplir con el licenciamiento de uso del respectivo módulos, componentes o librería.
- Los proveedores y terceros que desarrollen software para la UPIT y utilicen software de código abierto debe informar explícitamente a El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones los módulos, librerías o compontes que hayan utilizado.

5.29. Pruebas de seguridad y pruebas de aceptación

Todos de los nuevos desarrollos de software, actualizaciones, cambios o nuevas versiones de sistemas de información deben probarse y verificarse minuciosamente durante todo el ciclo de vida de su desarrollo, las pruebas de seguridad, análisis de vulnerabilidades y hacking ético deben ser parte integral del conjunto de pruebas que se deben ejecutar.

Todos los diferentes componentes del software o sistema de información deben ser sometidos a pruebas antes de su paso a producción, incluidos: sistema operacional, mecanismo de autenticación, controles de acceso a las funcionalidades del sistema, cifrado de datos, manejo de excepciones, validación de entradas y salidas, comunicaciones, así como módulos y librerías de terceros propiedad de terceros que hayan sido utilizados en el sistema.

Las pruebas de seguridad de los sistemas de información deben ser controladas mediante un plan de pruebas que considere responsable, acciones, resultados esperados, cronograma de trabajo y herramientas.

Se debe dar prioridad al uso de herramientas automatizada para realizar las pruebas del software, incluidas herramientas de análisis estático de código fuente, análisis

dinámico de código ejecutable, herramientas de análisis de vulnerabilidades y pruebas de carga.

Todo desarrollo de software debe ser sometido a pruebas de seguridad y a pruebas funcionales de aceptación. Las pruebas del software deben ser realizadas en un ambiente separado al ambiente de producción en el que se ejecutará el software.

Los datos para pruebas de sistemas de información y desarrollos de software de la UPIT no deben utilizar información de carácter personal real, cualquier dato personal usado en pruebas debe ser anonimizado antes de su uso en ambientes de prueba.

5.30. Desarrollo contratado externamente

Los desarrollos de software subcontratados deben:

- Ser supervisados para verificar que el proveedor esté aplicando prácticas de desarrollo seguro aceptadas por la UPIT.
- Contemplar cláusulas de cesión de derechos patrimoniales a favor de la UPIT.
- Ser sometidos a pruebas de seguridad y correcto funcionamiento supervisadas por el responsable de seguridad de la información del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.

Los contratos de desarrollo de software o sistemas de información para la UPIT deben incluir obligaciones de aplicación de prácticas de diseño, codificación y construcción segura.

Las pruebas de todos los desarrollos de software subcontratados por la UPIT deben ser controladas mediante un plan de pruebas que considere responsable, acciones, resultados esperados, cronograma de trabajo y herramientas.

Los datos de prueba para los desarrollos de software subcontratados por la UPIT no deben utilizar información no deben utilizar información de carácter personal real, cualquier dato personal usado en pruebas debe ser anonimizado antes de su uso en ambientes de prueba.

5.31. Separación de entorno de desarrollo, pruebas y producción

Los entornos de producción del software de los sistemas de información de la UPIT deben se diferentes a los entornos de desarrollo y pruebas del software.

Todos los proyectos de desarrollo de software de la UPIT deben establecer e implementar reglas para realizar el paso a producción de las versiones del software que ha superado satisfactoriamente las pruebas de seguridad y aceptación.

El paso a producción de nuevas versiones del software o sistemas de información debe realizarme aplicando un mecanismo de gestión de cambios controlados.

En los entornos de producción no deben estar disponibles herramientas, compiladores o programas utilitarios que permitan desarrollo de software no controlado.

El acceso a los entornos de producción debe ser limitado únicamente al personal encargado de los sistemas de información.

Los entornos de producción deben cumplir con la Política de Gestión de Vulnerabilidades Técnicas y la Política de Copias de la UPIT.

5.32. Gestión de cambios del software

Los cambios sobre las instalaciones de procesamiento de datos, servicios tecnológicos y sistemas de información se deben controlar a través de los mecanismos de gestión de cambios aprobados por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones y se deben gestionar durante la totalidad de su ciclo de vida: especificación, diseño, prueba, puesta en producción, retiro definitivo.

Todos los cambios en los ambientes de producción y pruebas deben incluir actividades de evaluación de los riesgos de seguridad de la información.

Todo desarrollo de software en la UPIT debe superar satisfactoriamente las pruebas de seguridad y aceptación antes de su paso a producción.

Todos los cambios en los ambientes de producción y desarrollo deben mantener registros de las modificaciones ejecutadas.

Los planes de continuidad y contingencia deben revisarse y actualizarse cuando se realicen cambios en los ambientes de producción y pruebas.

5.33. Información de pruebas

Los conjuntos de datos de prueba se deben preparar y mantener durante todo el ciclo de vida del desarrollo del software.

Los datos de prueba para los desarrollos de software de la UPIT no deben utilizar información de carácter personal real, cualquier dato personal usado en pruebas debe ser anonimizado antes de su uso en ambientes de prueba.

Los datos de pruebas se deben respaldar aplicando la política de copias de respaldo.

Los datos de pruebas para los sistemas de información deben considerar escenarios de datos erróneos y datos válidos.

5.34. Protección de los sistemas de información durante las pruebas

Las pruebas sobre los sistemas de información deben preservar la integridad y la disponibilidad de los sistemas de información y deben ser planificadas antes de su ejecución.

Se debe preferir la ejecución de las pruebas sobre los sistemas de información en ambientes controlados y no sobre los ambientes de producción.

5 Control de documentos

Versión Generada	Fecha	Descripción del Cambio o Modificación
01	08/08/2024	Creación del documento

Elaboró	Revisó	Aprobó
Juan Carlos Alarcón Suescún Contratista GIT de Gestión de Tecnologías de la Información y las Comunicaciones	**Bismark Benjamín Buenaños Mosquera** Coordinador GIT de Gestión de Tecnologías de la Información y las Comunicaciones	**Comité Institucional de Gestión y Desempeño** Sesión 08 de agosto de 2024