COMPENDIO DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá, septiembre de 2020

TABLA DE CONTENIDO

Listado de Ilustraciones

INTRODUCCIÓN

La Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD), en adelante la Unidad, como entidad pública es consciente de la importancia que representa su gestión, para el Gobierno Nacional, de servir de órgano administrativo para la restitución de tierras de los despojados. En dicha gestión está involucrada un tipo de población vulnerable, lo cual demanda una alta responsabilidad en cuanto al manejo adecuado de la información, puesto que no solamente se recolecta, administra y procesa información relacionada con los predios rurales abandonados a causa de la violencia, tales como: ubicación geográfica, relación jurídica con la tierra, actividades económicas desarrolladas en los predios abandonados y/o construcciones; sino que también se interactúa con datos personales, tales como: nombre, número de documento de identificación, cónyuge, entre otros; los cuales, en suma, constituyen una información de carácter sensible, que, aunque almacenada en una base de datos a cargo de la entidad, debe mantenerse reservada con miras a proteger los derechos fundamentales a la vida y a la integridad personal de la población víctima del desplazamiento forzado, pues se trata de datos "reveladores de realidades patrimoniales concretas que pueden ser fácilmente asociadas al nombre de una persona" y que, por lo mismo, son objeto de protección constitucional.

En atención a lo anterior, la entidad asumió el reto de implementar el Sistema de Gestión en Seguridad de la Información, en adelante SGSI, siguiendo las recomendaciones dispuestas en el Modelo de Seguridad y Privacidad de la Información (MSPI), basado en el Marco de Referencia de Arquitectura TI, el cual fue propuesto para el desarrollo de las arquitecturas empresariales sectoriales, institucionales y territoriales, convirtiéndose en el soporte de la Política de Gobierno Digital.

Las políticas complementarias de seguridad de la información identifican responsabilidades y establecen los objetivos para una protección apropiada de los activos de información de la entidad. La implementación de las políticas busca reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o usen en forma indebida los activos de información. Al mismo tiempo las políticas habilitan al subproceso de Seguridad de la Información en orientar y mejorar la administración de seguridad de los activos de información y proveer las bases para el monitoreo a través de toda la Unidad.

La seguridad comienza y termina con las personas, por tanto, las políticas:

- Son holísticas, es decir, cubren todos los aspectos relacionados con la misma.
- Se adecuan a las necesidades y recursos de la entidad.
- Son atemporales, es decir, el tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definen estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

Por tanto, cada política es revisada, aprobada, establecida y socializada desde la alta dirección a todos los niveles de la entidad, incluyendo servidores públicos, contratistas, proveedores y terceras partes, para su estricto cumplimiento.

1. OBJETIVO

Propender por el aseguramiento de la confidencialidad, integridad y disponibilidad de la información en la Unidad y sus partes interesadas a través de lineamientos que permitan mitigar riesgos de seguridad digital de acuerdo con lo dispuesto en la Política Nacional de Seguridad Digital y el Modelo de Seguridad y Privacidad de la Información.

2. OBJETIVOS ESPECÍFICOS

La presente política de seguridad de la información está orientada al cumplimiento de los siguientes objetivos específicos:

- Proteger la información de la Unidad y de los ciudadanos que acceden a los servicios de la entidad salvaguardando su confidencialidad, integridad, disponibilidad a través del establecimiento de políticas para mitigar los riesgos que vulneren los activos de información.
- Generar confianza en los ciudadanos, colaboradores y demás partes interesadas en el uso de los servicios de la Unidad.
- Gestionar y mitigar los riesgos que se puedan presentar para proteger los activos de información de la Unidad contra ataques, robo, intrusiones, accesos no autorizados y fuga de información, que afecten a la imagen, los intereses y el buen nombre de la Unidad.
- Establecer las responsabilidades y obligaciones de seguridad de la información en la Unidad.
- Mantener un nivel apropiado de concientización, conocimientos y habilidades necesarios para permitirles minimizar la ocurrencia de incidentes de seguridad de la información.
- Garantizar la continuidad del negocio frente a la ocurrencia de incidentes de seguridad de la información y eventos disruptivos.
- Definir las directrices basadas en el marco regulatorio y políticas vigentes.

3. ALCANCE

Las disposiciones contenidas en la política de seguridad de la información y las políticas complementarias aplican para todos los procesos identificados en la entidad (estratégicos, misionales, apoyo y control) que son soportados en la sede central, oficinas territoriales, y demás escenarios donde se desarrollen actividades de la Unidad como el teletrabajo y trabajo en casa, la gestión de proveedores y terceras partes interesadas, que dependan o interactúen con la Unidad.

Adicionalmente, aplica a toda la información creada, procesada y respaldada que soportan los diferentes procesos, sin importar el medio, formato, presentación o lugar en el cual se encuentre; incluyendo, pero no limitando a información:

- Almacenada en bases de datos, computadores, dispositivos de almacenamiento masivo.
- Respaldada en centros de datos.
- Almacenada en la nube Pública o Privada.
- Transmitida a través de redes públicas o privadas.
- Impresa o escrita a mano en papel o en tableros u otro medio semejante.
- Enviada por Scanner/fax o por cualquier otro medio similar.
- Archivo físico.
- Información grabada a través de los diferentes medios de comunicación y vigilancia.

4. DEFINICIONES

Ver definiciones en el listado de términos del sistema de información - STRATEGOS.

5. MARCO NORMATIVO APLICABLE

Ver la normatividad aplicable en el normograma del sistema de información - STRATEGOS.

6. CUMPLIMIENTO DE LA POLÍTICA

La política de seguridad de la información es de obligatorio cumplimiento. Cada colaborador y parte interesada debe entender y asumir su responsabilidad respecto a la administración de la información y de los activos que la soportan.

Cualquier incumplimiento de esta política que resulte comprometiendo la confidencialidad, integridad y disponibilidad de la información de la Unidad podrá generar sanciones de acuerdo con lo establecido por la normatividad vigente en Seguridad y Privacidad en Colombia y el Código de Integridad.

La política de seguridad de la información de la Unidad está acorde con las mejores prácticas definidas en ISO 27001:2013 y el Modelo de Seguridad y Privacidad de la Información, por tanto, cada colaborador, servidor público, contratista, proveedor o tercera parte interesada tomará las medidas aplicables para garantizar su cumplimiento.

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de la información hace parte del Sistema Integrado de Planeación y Gestión (SIPG) y se puede consultar en la intranet en el documento *MC-ES-05* POLÍTICA Y OBJETIVOS DEL SISTEMA INTEGRADO DE PLANEACIÓN Y GESTIÓN.

7.1. GOBIERNO Y ROLES DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se presentan los roles y el esquema de gobierno para la seguridad de la información en la Unidad:

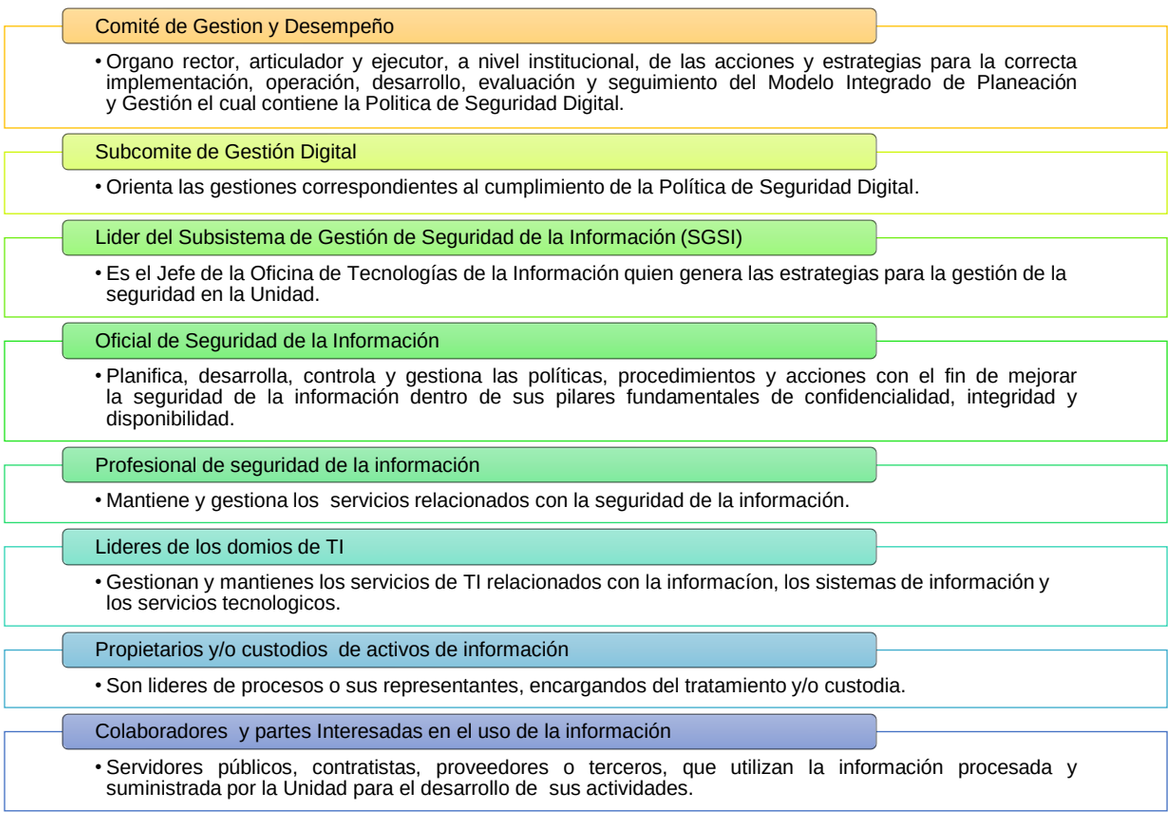

Ilustración 1. Roles de Seguridad de la Información
Fuente: OTI

7.2. POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas enunciadas a continuación se encuentran enmarcadas dentro del alcance definido en el numeral 3. ALCANCE, y se rigen bajo las normas y regulaciones del actual del gobierno de Colombia.

Cualquier excepción a las políticas complementarias de seguridad de la información debe seguir lo descrito en el numeral 9. EXCEPCIONES A LA PRESENTE POLÍTICA..

7.2.1. TELETRABAJO, TRABAJO EN CASA Y ACCESO REMOTO

La información a la que se tiene acceso y que es procesada o almacenada en los lugares en los que se realiza Teletrabajo, Trabajo en casa o Acceso Remoto, debe ser protegida para salvaguardar la confidencialidad y privacidad de esta. Todos los equipos de cómputo que sean usados en la modalidad de teletrabajo deben cumplir con los estándares de instalación y adecuación de seguridad de la información.

Lineamientos:

La Unidad debe:

a. Autorizar a los usuarios que dispondrán de la modalidad de teletrabajo, trabajo en casa o acceso remoto y brindar los permisos de acceso pertinentes; estos permisos deben estar aprobados por la entidad y se debe llevar control de los usuarios que trabajan bajo esta modalidad.
b. Llevar un seguimiento cercano de las conexiones remotas a los servicios corporativos de teletrabajo y trabajo en casa especialmente se debe prestar atención a los intentos de conexión que presenten comportamientos sospechosos.
c. Informar a los usuarios sobre como mitigar los riesgos asociados a la seguridad de la información.
d. Proporcionar una conexión segura a través de una VPN para acceder remotamente a los servicios que le permitan desarrollar las funciones designadas[1].
e. Denegar el acceso remoto al área de Tesorería y otras estaciones o sistemas que por su criticidad deban tener acceso presencial exclusivamente.

Los usuarios deben:

a. Verificar que sean cerradas todas las conexiones con servidores y páginas web, utilizando cuando sea posible la opción “desconectar” o “cerrar sesión”.
b. Establecer medidas en el sitio de teletrabajo/acceso remoto, para evitar el acceso fortuito a la información corporativa por otros usuarios del equipo (ej. familiares u otros), configurando contraseñas y cuentas de usuario, asi como el bloqueo automático por inactividad.
c. Contemplar las siguientes recomendaciones de protección frente al uso de equipos portátiles:
   - Utilizar guayas de seguridad.
   - Evitar transportar el equipo portátil sí no es necesario. En caso de ser transportado entre la oficina y el lugar de teletrabajo/acceso remoto, usar un maletín para protegerlo de caídas o golpes.
d. Si el usuario tiene cuenta de Office 365 brindada por la entidad, se deben almacenar los archivos de trabajo en la carpeta de One Drive.
e. Aplicar métodos para la destrucción segura de documentos físicos, evitando arrojarlos directamente al contenedor del reciclaje y/o evitar la reutilización para labores domésticas. Usar en lo posible una máquina de destructora papel o picar el papel en trozos pequeños que no permitan revelar la información.
f. Utilizar contraseñas robustas (que contengan números, letras y símbolos).
g. Los usuarios que realizan acceso remoto o trabajo en casa deben instalar Forticlient[1] para conectarse de manera segura al equipo de escritorio de la oficina y trabajar desde allí.

Los equipos de cómputo para usuarios de teletrabajo deben contar con las siguientes características:

a. Tener un sistema operativo y aplicaciones de trabajo licenciadas.
b. Tener un Software de antivirus legal, con la base de firmas actualizadas.
c. Si es un portátil y el sistema operativo cuenta con la opción de cifrado, se debe cifrar el disco duro donde se trabaja con la información de la entidad.
d. Parametrizar el bloqueo automático por inactividad.

[1] Ver en la intranet en el proceso de Gestión TI: Protocolo Configuración Cliente Forticlient y GT-PT-09 Protocolo de Conexión y Acceso - Trabajo en Casa

e. Manejar de cuentas de usuario independientes.

7.2.2. MEDIOS EXTRAÍBLES

La información que es almacenada en medios extraíbles debe protegerse y monitorearse para mitigar los riesgos asociados al acceso y divulgación no autorizada de la información.

Lineamientos:

a. Los puertos USB deben estar inhabilitados. Las excepciones deben estar autorizadas por la Oficina de Tecnologías de la Información.
b. Realizar el intercambio de información entre dependencias a través de las carpetas compartidas, con los permisos establecidos de acuerdo con la clasificación de la información.
c. El usuario debe eliminar la información que se encuentre en la carpeta pública (de traspaso de información) al terminar de compartir la información.
d. Analizar con el antivirus, los medios extraíbles cada vez que sean utilizados en los equipos de la entidad.
e. Instalar aplicaciones únicamente desde los repositorios oficiales provistos por la unidad.
f. Garantizar el cumplimiento de lo pactado en el acuerdo de confidencialidad sobre la información almacenada en los dispositivos extraíbles.
g. En lo posible cifrar los medios extraíbles y siempre guardar en un lugar seguro para evitar la pérdida o robo de la información.
h. No guardar información personal en los medios extraíbles asignados por la unidad.
i. No conectar los medios extraíbles en lugares que no ofrezcan las garantías de seguridad física necesarias para mitigar la pérdida o hurto de información de la Unidad.

7.2.3. GESTIÓN DE ACTIVOS DE INFORMACIÓN

Los activos de información se gestionan para establecer los límites y procedimientos frente a la identificación, uso, administración y responsabilidad de estos, indicando la necesidad, las prioridades y el grado esperado de protección al manejar la información. Por tanto, la Unidad debe definir controles para salvaguardar la información creada, procesada, transmitida y/o almacenada de sus procesos, con el fin de minimizar impactos financieros, operativos y/o legales debido al uso incorrecto de la información.

Lineamientos:

a. Los propietarios de los activos de información (Lideres de Proceso) deben encargarse de la identificación, actualización, valoración y clasificación en el inventario de los activos de información, de acuerdo con la metodología establecida para tal fin. Esta actividad debe realizarse como mínimo una vez al año.
b. Se debe prever que los activos de información críticos se encuentren localizados en áreas seguras y debidamente protegidos contra amenazas que puedan afectar su buen uso, disponibilidad y confidencialidad.
c. Los activos de información críticos que sean de tipo digital deben estar protegidos con una contraseña.
d. Se deben establecer controles o medidas acordes con la valoración de los activos de información y los riesgos asociados.
e. Los colaboradores deben almacenar siempre la información digital de la entidad ubicaciones donde se esté respaldando la información.
f. La metodología para identificar, valorar y clasificar los activos de información se desarrolla en el documento de GT-GU-12 METODOLOGÍA DE IDENTIFICACIÓN, VALORACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN
g. Se debe contar con una autorización escrita para el retiro de activos críticos de información de la entidad, así como la firma del acuerdo de confidencialidad.

7.2.4. CONTROL DE ACCESO

La Unidad debe implementar controles de acceso a los activos de información, con el fin de otorgar acceso solo por personas y medios autorizados, determinando mecanismos de protección, límites y procedimientos frente a la administración de accesos electrónicos o físicos.

Lineamientos:

Responsabilidades de los colaboradores y demás partes interesadas.

a. Proteger las credenciales asignadas para el acceso y uso de los servicios tecnológicos, así como el ingreso a áreas seguras, las cuales deben ser personales e intransferibles.
b. Suscribir un Acuerdo de Confidencialidad, con lo cual respalda[2] su responsabilidad y compromiso frente a no divulgar la información interna y externa que conozca de la Entidad, y demás relacionadas con en el ejercicio de sus funciones.
c. Restringir el acceso a oficinas, salas de telecomunicaciones, servidores y áreas de trabajo que contengan información clasificada y/o reservada, concediendo el ingreso bajo autorización previa del propietario de la información.
d. El ingreso de visitantes debe cumplir el procedimiento aprobado por la Unidad.
e. Todos los sistemas deben restringir su acceso mediante un método de autenticación. Crear contraseñas robustas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la entidad. Crear contraseñas robustas con las siguientes características, si el sistema no obliga a cumplir las siguientes políticas, los usuarios deben hacerlo manualmente:
    - Longitud mínima de 8 caracteres
    - Solicitar cambio de contraseña con una periodicidad mensual.
    - La contraseña no podrá ser equivalente a las 12 últimas contraseñas anteriores.
    - La contraseña debe contener mínimo una letra mayúscula, un número y un carácter no alfanumérico.
    - La contraseña no debe contener parcialmente el nombre de usuario.
f. Los colaboradores que requieran acceder remotamente vía VPN se debe hacer uso del doble factor de autenticación siempre y cuando exista esta función.
g. Acceder a la información y a las aplicaciones de un sistema de información solo cuando haya sido autorizado formalmente por el propietario de la información.
h. Asegurar todas las áreas físicas acorde con el valor de la información que allí procesa, almacena y trasmita. Los sitios restringidos como cuartos técnicos o cualquier otro lugar donde se procese información deben tener controles de acceso.
i. Evitar el uso compartido de cuentas de usuario y sus contraseñas. La autenticación en la plataforma tecnológica debe ser única y personalizada. Solo se permitirán cuentas de grupos en casos excepcionales como cuentas de correo que representan a las dependencias o en sistemas de información para el envío de notificaciones o que por su funcionalidad lo requieran.

Responsabilidad del propietario del activo de la Información (Lideres de los procesos).

a. Los líderes de proceso o a quien designe deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, firmando el formato GT-FO-14 GESTIÓN DE CREDENCIALES.

[2] *La responsabilidad por el manejo de información confidencial de víctimas de violaciones al Derecho Internacional Humanitario (DIH) se entiende configurada por el hecho de manejarla, en concordancia con la Declaración sobre los Principios Fundamentals de Justicia para las Victimas, adoptada por la Asamblea General de la Organización de Naciones Unidas, en Resolución 40/34 de 29 de noviembre de 1985, numeral 6°, y la Sentencia de la Corte Constitucional T-1135 de catorce (14) de Noviembre de 2008, M.P. Dr. Manuel Jose Cepeda Espinosa.*

Responsabilidades de los colaboradores y proveedores que realizan tareas de administración de sistemas de información y bases de datos

j. Establecer las medidas de control de acceso de los servidores públicos y contratistas, a través de mecanismos de identificación, autenticación y autorización de acceso, a nivel de sistemas de información, Bases de Datos y servicios de TI de acuerdo con los perfiles y cargos instaurados en la entidad.
k. Verificar los controles de acceso de los servidores públicos y contratistas, de manera mensual, a fin de validar que los usuarios accedan solamente a los recursos autorizados para la realización de sus tareas; inactivando los accesos de los usuarios que han sido retirados de la Unidad.
l. Garantizar que el administrador de cada sistema, aplicativo o dispositivo de la Infraestructura Tecnológica, proporcione a su jefe inmediato o supervisor, las contraseñas de administración.
m. Validar periódicamente que solo se encuentran activos los usuarios autorizados para los diferentes sistemas.
n. Crear contraseñas robustas con las siguientes características, si el sistema no obliga a cumplir las siguientes políticas, los usuarios deben hacerlo manualmente:
    - Longitud mínima de 10 caracteres
    - Solicitar cambio de contraseña con una periodicidad mensual.
    - La contraseña no podrá ser equivalente a las 12 últimas contraseñas anteriores.
    - La contraseña debe contener mínimo una letra mayúscula, un número y un carácter no alfanumérico.
    - La contraseña no debe contener parcialmente el nombre de usuario.

Responsabilidad de Servicios Tecnológicos y personal de Soporte Técnico

a. Separar los ambientes de desarrollo, pruebas y producción.
b. Controlar los cambios en los ambientes de producción los cuales deben estar debidamente autorizados.
c. Asegurar que los grupos de servicios de información, usuarios y sistemas de información sean segregados en redes independientes.
d. Asegurar que las redes inalámbricas cuenten con métodos de autenticación que evite accesos no autorizados.
e. Todos los sistemas (servidores, equipos activos de red y máquinas de usuarios) deben contar con sincronización de reloj a nivel de sistema operativo, teniendo como referencia la Hora Legal Colombiana. No está permitida la desactivación del sistema de sincronización o la manipulación manual de la hora.
f. Todos los equipos de cómputo de la Entidad deben tener instalados los parches de seguridad más recientes proporcionados por los fabricantes.
g. Todos los equipos de cómputo de la Entidad deben tener instalado software de protección contra malware.
h. Proteger con un dispositivo de alimentación de energía ininterrumpida (UPS) de uso exclusivo para cada estación de procesamiento crítico de información.
i. Deben habilitarse sólo los servicios y funcionalidades del sistema que corresponda, bajo el principio de menor privilegio[3].
j. Los servicios de procesamiento de información sensible para la Unidad deben estar ubicados en áreas seguras y protegidas por controles de acceso adecuados.
k. Diseñar y gestionar la red de datos siguiendo las normativas internacionales de cableado estructurado. En consecuencia, está prohibido (salvo autorización o supervisión expresa de la OTI) la intervención física de los usuarios sobre los recursos de la red institucional (cables, enlaces, estaciones de trabajo, dispositivos de red).
l. Los centros de procesamiento de datos o unidades de procesos críticos deben tener zonas restringidas, únicamente accesibles por personal autorizado.
m. Configurar que el inicio de las estaciones y servidores se haga siempre desde el disco duro, se debe asignar una clave al BIOS de cada estación con el finde prevenir la configuración de inicio desde medios extraíbles, el acceso al sistema operativo debe efectuarse a través de una clave de dominio.
n. Realizar el soporte técnico, actualización y mantenimiento a las estaciones de trabajo y servidores de la entidad acorde a las especificaciones de los fabricantes del equipo.

[3] Es una estrategia de seguridad, aplicable a distintos ámbitos, que se apoya en la idea de otorgar únicamente permisos cuando son necesarios para el desempeño de cierta actividad.

Responsabilidad de Seguridad de la Información

o. No se permite ninguna conexión directa de entrada o salida de tráfico entre Internet y la red de la Entidad.
p. Los sistemas que proporcionan servicios de acceso público deben ubicarse dentro de un esquema de zona desmilitarizada que permita limitar el tráfico.
q. Siempre debe existir un firewall en cada conexión a Internet y entre cualquier zona desmilitarizada y la zona interna de la red.
r. Todo cambio en la configuración de firewalls y routers debe seguir el procedimiento definido de control de cambios.
s. Se debe mantener actualizados de los servicios, protocolos y puertos abiertos en el firewall.
t. Realizar revisiones periódicas de la configuración del firewall.
u. Revisar, aprobar o rechazar la solicitud de conexión remota (VPN); los cuales deben estar soportados y avalados por el jefe o supervisor del colaborador que hace la solicitud.

7.2.5. USO DE COMPUTADORES PERSONALES – (BYOD, Bring your own Device)

Los colaboradores y terceros que por sus labores requieren tener acceso a los recursos de información de la entidad a través de sus computadores personales, deben aceptar las políticas y controles que se establezcan con el fin de proteger los activos de información a los cuales acceden. No deben existir dispositivos con información de la entidad que no cuenten con los lineamientos definidos por la Unidad.

Lineamientos:

a. La información que pueden visualizar los colaboradores y terceros a través de los dispositivos que ingresen a la Unidad es confidencial y de uso exclusivo para el desarrollo de sus labores dentro de la entidad.
b. La configuración de este servicio en los dispositivos de los colaboradores y terceros de la Unidad se debe realizar únicamente a quienes dadas sus obligaciones requieran del uso de este servicio.
c. Los colaboradores y terceros deben firmar el formato GT-FO-32 ACEPTACIÓN DE LA POLÍTICA COMPLEMENTARIA PARA EL USO DE DISPOSITIVOS PERSONALES en donde expresan que entienden, aceptan y se comprometen a cumplir las Políticas de Seguridad de la Información de la Unidad.
d. Los dispositivos deben ser validados por el personal de soporte de la Unidad con el fin de garantizar que cuenten con un Antivirus Legal; adicionalmente se debe registrar la información básica para identificar el dispositivo como lo son: marca, modelo, serial, sistema operativo, antivirus y MAC.
e. Los colaboradores y terceros son responsables de salvaguardar toda la información que se almacena en sus dispositivos, la Unidad no se hace responsable por la realización de copias de respaldo. Así mismo, son responsables de la eliminación y entrega de la información propia de la Unidad en el momento de la desvinculación o terminación del contrato.
f. Los dispositivos que no hacen parte de la Unidad, no se encuentran cubiertos por el alcance del servicio de soporte técnico. Cualquier tipo de mantenimiento o reparación por daño es responsabilidad del propietario.
g. La Unidad se reserva el derecho de monitorear y restringir las actividades que puedan vulnerar la confidencialidad, integridad y disponibilidad de la información. Así como remover los derechos de acceso a los sistemas y la información en el momento de la desvinculación, terminación del contrato o por solicitud unilateral de la OTI.

7.2.6. DISPOSITIVOS MÓVILES DE LA ENTIDAD

La configuración de los dispositivos asignados a los colaboradores de la entidad se debe realizar únicamente para quienes por su cargo y obligaciones requieran de la asignación de un dispositivo móvil. Es responsabilidad del colaborador hacer buen uso de la información de la entidad que reposa en los dispositivos asignados.

Lineamientos:

a. Bloquear el dispositivo a través de un método de contraseña y se debe configurar para que se habilite en un periodo de inactividad.
b. Mantener actualizada la versión del sistema operativo del dispositivo.
c. Conectarse a redes inalámbricas seguras.
d. En la medida que el sistema operativo lo permita se recomienda cifrar el dispositivo.

Nota: Para el caso de teléfonos inteligentes o tabletas que no son de propiedad de la Unidad, se permitirá a los colaboradores el acceso a los servicios de Microsoft 365

7.2.7. PORT SECURITY (PUERTO SEGURO DE RED)

El usuario es responsable de la seguridad de su puesto de trabajo y el equipo de cómputo asignado para ejercer sus funciones en la Unidad.

Lineamientos:

El puesto de trabajo incluye un punto de red para que el equipo asignado al usuario se conecte a la red de datos, a este punto de red solo se permitirá la conexión de los equipos previamente validados por el área de soporte técnico de la OTI. No se permitirá el movimiento de equipos de cómputo sin previo aviso a la OTI, responsable por la administración de los recursos tecnológicos, para que realice la configuración del nuevo punto de red. Si se conecta un equipo que no ha sido validado por la OTI el punto de acceso se inhabilitara por seguridad.

7.2.8. RESPALDO Y RECUPERACION

Se deben almacenar en lugares seguros las copias de respaldo de los recursos críticos de acuerdo con su clasificación y garantizar las medidas de protección adecuadas, dependiendo de la criticidad de los activos de información identificados.

Lineamientos:

a. Realizar copias de seguridad sobre los activos que se consideren necesarios de acuerdo con la criticidad, asegurándose de tener la capacidad de restaurar de forma completa y oportuna la información en caso de requerirla.
b. Definir y mantener los procedimientos de respaldo, así como las herramientas tecnológicas necesarias.[4]
c. En la medida que sea posible y dependiendo de la valoración del activo de información se recomienda cifrar la información con el fin de velar por el principio de confidencialidad.
d. Se deben realizar pruebas de restauración de copias de seguridad para activos críticos.
e. Generar informes sobre los resultados de las copias de seguridad.
f. Los dispositivos usados para el respaldo de la información deben ser monitoreados para mantener el estado de salud de la plataforma.

7.2.9. CONTROLES CRIPTOGRÁFICOS

De acuerdo con el valor y criticidad de cada uno de los activos de información se deben establecer controles que protejan la información respaldada y transmitida haciendo uso apropiado y eficiente de la criptografía, a fin de proteger la confidencialidad de la información.

[4] Ver GT-IN-03 INSTRUCTIVO PARA COPIAS DE SEGURIDAD Y RECUPERACION EN SERVIDORES

Lineamientos:

a. Utilizar controles criptográficos como el cifrado para proteger la información crítica, así como el nivel o fortaleza de los mecanismos de cifrado a utilizar de acuerdo con el tipo de información (algoritmos, longitudes de clave mínimas, etc.).
b. Las claves, tokens, certificados SSL y firmas digitales deben guardarse en lugares seguros, los medios digitales deben contar con respaldos periódicos.
c. Tener en cuenta los siguientes aspectos para la definición de los criterios criptográficos:
    - Contar con herramientas y mecanismos de cifrado simétricos y asimétricos (Certificados SSL) en la entidad.
    - La sensibilidad de la información y su nivel de clasificación, así como los sistemas y líneas de comunicaciones por los que se almacena, procesa o transmite la información.
    - La gestión de claves: generación, almacenamiento, renovación, revocación, etc.
    - Recuperación de la información cifrada en caso de pérdida o destrucción de las claves.
d. Los administradores de infraestructura y de sistemas deben usar la herramienta Keepass[5] para la gestión de las claves, así como hacer la entrega de la clave maestra al jefe o supervisor para que la custodie y en un caso fortuito una tercera parte autorizada pueda tener acceso para poder descifrar los datos.
e. Cuando se compartan claves, se debe garantizar la confidencialidad en el intercambio de las claves por un canal seguro y diferente al que se envía la información cuando exista transferencia de la misma.
   Hacer uso de certificados SSL para los aplicativos que se encuentran expuestos a internet, en lo posible y de acuerdo con la disponibilidad de certificados realizar lo mismo para los servicios internos.

7.2.10. ESCRITORIO LIMPIO Y PANTALLA LIMPIA

El escritorio y la pantalla se deben mantener limpios de cuadernos, post-it, documentos y medios de almacenamiento removibles, los cuales deben estar almacenados en un lugar seguro.

Lineamientos:

a. Mantener su escritorio físico limpio y organizado: Si este se encuentra desordenado, es muy probable que no se pueda identificar la pérdida de algún elemento. Los documentos de la Entidad deben estar disponibles únicamente a personas autorizadas y bajo la responsabilidad del custodio que salvaguarda la información.
b. Mantener la pantalla y escritorio limpio, libre de iconos y/o accesos directos innecesarios: Las estaciones de trabajo, equipos portátiles y computadores de escritorio deben tener el fondo de escritorio y protector de pantalla institucional, de forma que se active ante un tiempo específico sin uso. Al ingresar a la cuenta, la pantalla debe solicitar únicamente el nombre de usuario y contraseña.
c. Proteger la información que se manipula diariamente, así como los elementos de procesamiento y demás fuentes de datos físicos.
d. Recoger, almacenar y asegurar bajo llave el material físico al finalizar la jornada de trabajo y/o cuando se ausente de su puesto de trabajo, no deben reposar carpetas, ni oficios en los escritorios, estos deben ser salvaguardados bajo llave; de igual manera, una vez se impriman documentos, estos deben ser retirados inmediatamente de las impresoras.
e. Bloquear el equipo de cómputo cuando se retire de su puesto de trabajo: Es importante que los equipos portátiles y computadores de escritorio sean bloqueados cuando el colaborador se retire de su lugar de trabajo.
f. Se debe programar el bloqueo automático de la sesión a 5 minutos por inactividad.

7.2.11. TRANSFERENCIA DE INFORMACIÓN

Salvaguardar la información transferida dentro de la entidad y con cualquier entidad externa.

[5] Ver en intranet el proceso Gestión TI - Protocolo para el uso del gestor de contraseñas Keepass.

Lineamientos para el intercambio de información con otras entidades:

a. Se deben seguir los lineamientos de seguridad establecidos en el modelo de interoperabilidad definido en la Unidad, con el fin de garantizar la Confidencialidad, Integridad, Disponibilidad, Autenticación, Autorización, Auditoria, y el No Repudio, que se requiere para el intercambio seguro de datos.
b. Las transferencias de información realizadas en la Unidad deben tener registros que permitan su trazabilidad. Como mínimo se debe mantener registro de:

- Fecha y Hora
- Dirección IP
- Usuario
- Transmisión exitosa / fallida.
- Tamaño de los datos transmitidos.
- Algoritmo de cifrado o firmado.

6.2.12. DESARROLLO SEGURO

Garantizar que la seguridad sea parte integral de los Sistemas de Información durante todo el ciclo de vida, diseño, implementación, desarrollo y pruebas.

Lineamientos:

a. La privacidad, confidencialidad e integridad del activo de información con base en el nivel al que pertenezca el mismo y el nivel de evaluación de riesgo, se debe salvaguardar, por tanto, se debe considerar:
   - **Cifrado de datos clasificados como reserva:** Los datos en tránsito entre diferentes sistemas y el almacenamiento de esta información se deben cifrar con un algoritmo criptográfico. Usar HTTPS para aplicaciones web.
   - **Control de acceso:** Mecanismos de autenticación por usuario y contraseña siguiendo la Política de control de acceso a la información establecida en este documento
   - **Registro**: Registrar eventos que evidencien las acciones realizadas con el fin de tener un registro de auditoria de las acciones que realiza el usuario.
   - **Validar la integridad de los datos:** Implementar opciones que permitan validar la integridad de los datos almacenados y/o transmitidos dependiendo de su criticidad utilizando opciones como por ejemplo: un campo de hashing que se genera con un algoritmo seguro que será calculado en la capa de acceso a datos con el uso de una librería validada. Este valor será almacenado hasta el momento en que se requiera la validación de integridad, momento en que se volverá a calcular el hashing y se realizará la comparación con el valor almacenado anteriormente.

b. El no repudio se debe establecer a través de la habilitación de los registros de auditoria, cuando se realizan las siguientes acciones:
   - Creación, modificación y/o eliminación de datos.
   - Creación, modificación y/o eliminación de usuarios.
   - Creación, modificación y/o eliminación de perfiles de usuario.
   - Cambios en la configuración de la aplicación.

c. Los datos a registrar para tener trazabilidad de las acciones desarrolladas en los sistemas de información deben ser:
   - **Fecha y Hora:** Señalando el año, mes, día, hora, segundos y milisegundos de la recepción del requerimiento.
   - **Usuario:** Identificación de la cuenta responsable de la acción.
   - **Tipo de requerimiento o servicio:** Señalar cual fue la acción solicitada por el usuario (adición, eliminación, consulta, etc.)
   - **Id:** Identificador de la transacción.

- **Estado:** Indica si fue exitosa o no la transacción.

De ser posible registrar los siguientes elementos:

- **Problema Identificado:** Si la transacción no fue exitosa, especificar la causa correspondiente como problemas en la conexión, no hay respuesta de la Base de Datos, problemas en el enlace; se utilizará el mismo mecanismo descrito en el campo de Alerta.
- **Registro afectado:** ID del registro objetivo de la acción del usuario
- **Base de Datos:** ID de la Base de Datos afectada por la acción del usuario
- **Tabla:** ID de la tabla afectada por la acción del usuario
- **Tamaño de la trama:** En las transferencias de información. Registrar el tamaño del mensaje enviado para la solicitud
- **Tamaño de la trama de respuesta:** En las transferencias de información. Registrar el tamaño del mensaje que la aplicación respondió

d. Los datos de entrada deben ser validados, si hay carencias en esta funcionalidad, se presentarán vulnerabilidades de inyección o buffer overflow, que pueden causar ataques de negación de servicio que afecten la disponibilidad o accesos no autorizados que comprometen la integridad y/o confidencialidad de la información. En el desarrollo de la aplicación se deben tener en cuenta las siguientes consideraciones:

- **Protección contra buffer overflow:** Aplicación de las mejores prácticas en el desarrollo para tener un estricto control en la definición del tipo de variables para que se ajusten a los requerimientos. La validación se realiza analizando el código en cada una de las sentencias de definición de variables para que se limiten a un dominio o rango requerido por la función correspondiente. Considerando lo anterior, cada variable definida debe tener un tipo de datos limitado, preferiblemente definido por el programador y que los mecanismos sean diseñados para que solo capturen lo estipulado por los formatos aceptados o lo estrictamente requerido. Por ejemplo, si se va a capturar un número celular, la variable definida debe ser un campo tipo texto de 10 caracteres y cuando se capture dicho campo se debe validar que solo se acepten valores entre 0 y 9 y que la entrada solo puede ser de 10 caracteres rechazando cadenas de texto de menor o mayor longitud; si dentro de la revisión de código se evidencia que no se implementan estas restricciones, a pesar de que funcionalmente sea aprobado se está generando una vulnerabilidad.
- **Restricción de las capturas:** Los datos que se ingresen al sistema estarán restringidos por la longitud y el tipo de datos para limitar a lo estrictamente necesarios.
- **Librerías:** Evitar el uso de librerías con vulnerabilidades de cualquier tipo.
- **Parámetros pasados a través de la URL:** Restringir el tamaño y el tipo de caracteres que son pasados en los parámetros de la URL para evitar ataques y la exploración no autorizada de directorios del servidor donde resida la aplicación.

e. El manejo de excepciones en el desarrollo de los sistemas de información para cada una de las funciones implementadas, deben contemplarse las opciones resultantes de los casos de abuso, es decir evitar que la aplicación pierda el control en el flujo posible de acciones, evitando que una excepción permita violar las políticas de seguridad definidas. Todas las funciones tendrán un manejo específico para los casos que estén por fuera de los que señalan los requerimientos funcionales. Las transacciones deben garantizar el componente de atomicidad.

7.2.13. CONSERVACIÓN Y DESTRUCCIÓN DE LA INFORMACIÓN

Es responsabilidad del dueño del activo de información, determinar cuando la información ha dejado de ser útil para la Entidad de acuerdo con su valoración y acorde a la regulación que aplique.

<u>Lineamientos:</u>

a. Se deben establecer procedimientos relacionados con el tratamiento de la información durante su vida útil y usar mecanismos de destrucción o borrado seguro de acuerdo con el medio que la custodie.
b. Todos los colaboradores deben destruir de manera segura los documentos físicos clasificados como de Uso Clasificado/Reservado previo a su desecho (con máquina trituradora).
c. Asegurar y legalizar la devolución del activo que estaba bajo la responsabilidad del contratista o servidor público, antes de su desvinculación.
d. Ejecutar un borrado seguro de los medios de almacenamiento de información asignados[6] a fin de evitar la recuperación de la información; actividad que debe ser ejecutada por el Área de Soporte de la OTI y aprobada por el Oficial de Seguridad de la Información.

7.2.14. USO ADECUADO DEL CORREO ELECTRÓNICO CORPORATIVO

Está prohibido el uso del correo electrónico corporativo para asuntos diferentes a los relacionados con la misión y actividades relacionados con la entidad. Algunos ejemplos de eventos de riesgo relacionados que pueden afectar la seguridad de la información son:

- Fuga de información.
- Proliferación de malware (virus).
- Pérdida de la confidencialidad de la información.

Lineamientos:

a. Mientras la capacidad de licenciamiento lo permita se debe asignar una cuenta de correo electrónico nombrada con el estándar *primernombre.primerapellido@restituciondetierras.gov.co* a los colaboradores de la entidad. Si ya existe se debe crear segundonombre.primerapellido@restitucion*detierras.gov.co*
b. Las cuentas personales de correo electrónico (Yahoo, Hotmail, Gmail, etc.), deben estar bloqueadas en los equipos de la Unidad. Las excepciones para hacer uso de correo personal deben ser documentadas y justificadas.
c. Las cuentas de correo electrónico son personales y de uso exclusivo para el desarrollo de las funciones de cada uno de los colaboradores; por lo tanto, la información gestionada a través de este medio es responsabilidad de cada usuario y debe cumplir con las condiciones de confidencialidad, integridad y disponibilidad reglamentadas en esta política. La información gestionada a través de este medio es propiedad de la entidad.
d. Con el fin de propender por la movilidad y productividad se permitirá el acceso al correo electrónico desde cualquier lugar a través de internet, siempre y cuando se tenga presente el cuidado de los activos de información que estén bajo su responsabilidad.

No es permitido:

a. El envío o recepción de archivos ejecutables. (ej. exe, bat, etc.)
b. Utilizar el correo electrónico para el envío de cadenas de correo, mensajes con contenido religioso, político, racista, pornográfico o cualquier tipo de mensaje que atente contra la integridad de las personas, las leyes y la moral. El correo electrónico institucional no debe usarse para actividades que comprometan la reputación de la entidad, los activos de información y los recursos de la Unidad.
c. Enviar mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
d. Utilizar la dirección de correo electrónico de la Unidad como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, Twitter, Instagram, entre otras, o cualquier otro sitio, a menos que sea utilizado con fines de comunicación, representación en eventos y publicaciones oficiales de la entidad.
e. Enviar información clasificada o reservada a cuentas personales.

[6] Ver PROTOCOLO PARA EL BORRADO SEGURO DE LA INFORMACION PARA EQUIPOS ALQUILADOS SIN RECUPERACIÓN

f. Enviar información clasificada o reservada a otras entidades sin la autorización escrita correspondiente.

7.2.15. SEGURIDAD FÍSICA

Ingreso de visitantes

Lineamientos:

Todos los visitantes deben pasar el procedimiento de identificación en la recepción y deben ser recibidos por un colaborador para el acompañamiento obligatorio dentro de las instalaciones, en cumplimiento de los procedimientos establecidos en el proceso de gestión logística y recursos físicos y los lineamientos emitidos por el Grupo de Gestión de Seguimiento y Operación Administrativa.

El cumplimiento del procedimiento de Control de acceso físico es responsabilidad de todos los colaboradores al asegurar el acompañamiento de sus visitantes en las instalaciones de la entidad

Acceso a las instalaciones y oficinas

Lineamientos:

Las áreas donde se ejecutan procesos relacionados con información confidencial o restringida deben contar con controles de acceso que sólo permitan el ingreso a los colaboradores autorizados.

Áreas restringidas: deben contar con mecanismos que permitan restringir el acceso sólo a personal autorizado y que permita guardar la trazabilidad de los ingresos y salidas. Los colaboradores que tienen acceso a estas áreas son responsables de proteger la identificación que le otorga estas facultades y responder por los actos que se cometan con su identificación y en los que se evidencie negligencia o descuido de sus credenciales o claves de ingreso.

Cámaras de video

Lineamientos:

Se deben instalar y monitorear cámaras de video en sitios estratégicos que permitan realizar seguimiento al cumplimiento de las políticas de seguridad física. Las imágenes deben ser conservadas por un tiempo que sea establecido localmente en cada uno de los lugares de trabajo, o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

La instalación de las cámaras debe ser acorde a la identificación de áreas sensibles y las imágenes se deben monitorear con el fin de identificar situaciones que requieran la ejecución de acciones disciplinarias o de mejoramiento.

Esquema de vigilancia

Lineamientos:

La Unidad debe gestionar el diseño, monitoreo y mantenimiento de un esquema de vigilancia que permita garantizar el cumplimiento de las políticas de seguridad física, salvaguardar los activos de información de la entidad y proteger la integridad de los colaboradores y visitantes.

Se debe mantener un esquema de vigilancia acorde con las necesidades de seguridad de la información de la Unidad, el cual debe ser valorado y ajustado periódicamente.

7.2.16. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Garantizar que se tomen acciones correctivas de los incidentes de seguridad de la información que se reportan y se documentan de manera oportuna; dicha política se desarrolla en el documento *GT-MA-05 POLÍTICA DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*

7.2.17. TRATAMIENTO DE DATOS PERSONALES

EL objetivo de la POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DE LA UNIDAD ADMINISTRATIVA ESPECIAL DE GESTIÓN DE RESTITUCIÓN DE TIERRAS DESPOJADAS, es cumplir y garantizar la aplicación de la normatividad correspondiente a la protección de datos personales vigente, con el fin de dar un correcto tratamiento a los mismos, por lo que se procede a establecer los deberes, derechos y responsabilidades de las partes, así como el procedimiento para realizar la autorización de uso de la información, consultas y reclamos de los titulares de los Datos Personales y demás actividades propias que se pueden desarrollar con ocasión de esta política, la cual se desarrolla en el documento *GT-MA-06 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES.*

7.2.18. USO DE CARPETAS COMPARTIDAS

Para usuarios:

a. Limpiar regularmente la carpeta compartida de la dependencia, así como su carpeta personal en la red, eliminando la información que no se requiera.
b. Evitar colocar archivos de vídeo o aplicaciones no autorizadas o que infrinjan la Ley de Derechos de Autor y Propiedad Intelectual.
c. Comprimir las carpetas que contengan gran cantidad de archivos. Esto facilita la realización de las copias de seguridad.
d. Los respaldos de información se guardarán de acuerdo con lo establecido en el *INSTRUCTIVO PARA COPIAS DE SEGURIDAD Y RECUPERACION EN SERVIDORES*.
e. De requerir más espacio en las carpetas personales (nombre.apellido) se debe hacer la solicitud a la OTI mediante un GLPI.
f. Los recursos son compartidos, el mal uso de estos servicios afecta al resto de usuarios, por lo tanto, no se debe duplicar la información y se deben mantener fuentes únicas de información.

Para administradores:

a. Las carpetas donde reposan los archivos escaneados solo deben mantener la información del último mes el resto deben ser eliminadas.
b. Asignar permisos sobre carpetas compartidas a grupos de usuario. Excepto las carpetas personales (nombre.apellido) a las que se le realizara backup.
c. Deshabilitar los usuarios "invitado".
d. Para actividades regulares de administración del servidor no utilizar la cuenta de administrador, se debe custodiar con una contraseña compleja que sea cambiada periódicamente.
e. Crear cuentas de administración nombradas sin que tengan la palabra admin o similar, para que el nombre de usuario no indique sus privilegios (Ej: nombre.apellido1)
   Limitar los privilegios de grupos de usuarios por defecto, existen carpetas compartidas para los usuarios del sistema operativo, así como grupos como “Everyone”.
f. Desactivar la opción de mostrar el último usuario en la pantalla de inicio o bloqueo del sistema.
g. Habilitar la protección de los archivos de registro de eventos. Por defecto este tipo de archivos no se encuentran protegidos, es importante dar permisos de lectura como de escritura a usuarios del sistema y administradores, de lo contrario un atacante podría fácilmente eliminar sus registros luego de un ataque.

7.2.19. USO ADECUADO DEL INTERNET

El acceso a Internet en la entidad responde a la utilización de una herramienta de uso estrictamente laboral. Para estos efectos, cualquier propósito ajeno a las funciones estrictamente laborales serán restringidas.

Lineamientos:

a. Los privilegios de uso de Internet estarán definidos de acuerdo con la necesidad de acceso que requiera el desarrollo de la función de cada usuario y que vayan acordes con los procesos que gestionan, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.
b. Los colaboradores y/o terceros, no pueden asumir en nombre de la Unidad, posiciones personales en encuestas de opinión, foros u otros accesos web similares.
c. Está estrictamente prohibido el ingreso a Páginas Web con contenido que se considere inapropiado, ofensivo, ilegal o que pueda atentar contra la seguridad de la información.
d. El usuario no debe descargar ningún programa o software, sin la debida autorización, de la Oficina de Tecnologías de la Información.
e. El manejo de información a través la nube únicamente está autorizado a través de la herramienta *One Drive*.
f. Cualquier cambio o excepción deberá estar soportado y con las aprobaciones respectivas.

7.2.20. ASEGURAMIENTO AREA DE TESORERIA

Se deben fortalecer los controles para los equipos donde se realizan transacciones financieras con el objeto de minimizar la probabilidad de fraude en la gestión de las operaciones de liquidez, transacciones de valores, pagos por archivos planos y dispersiones desde los portales bancarios con dineros que se solicitan con traspaso a pagaduría.

Lineamientos:

Cámaras de Seguridad:

a. De acuerdo con las condiciones físicas de la entidad, las instalaciones de la tesorería deben contar con cámaras de video ubicadas en los corredores de acceso y al interior del área de tesorería.
b. Las cámaras de video deben ser ubicadas de forma tal que no permita visualizar teclados, monitores y deben identificar al funcionario que hace uso de los dispositivos.
c. Deben visualizar la caja fuerte.
d. Deben ser monitoreadas constantemente por la empresa de vigilancia y seguridad a cargo.
e. Se debe mantener las grabaciones en custodia de los videos y acorde con los tiempos de retención definidos por la entidad.

Caja Fuerte:

a. La caja fuerte debe estar dentro de Tesorería y será manipulada única y exclusivamente por el (la) Tesorero (a) a cargo.
b. La clave debe ser custodiada por el tesorero y se debe cambiar periódicamente o en caso de que se sospeche que haya sido revelada, también se debe gestionar la entrega en caso de ausencias como vacaciones, retiro, entre otros.

Talento Humano:

c. Se debe tener definido claramente el perfil, la experiencia y las competencias adecuadas para los cargos vinculados a la Tesorería.
d. Los cargos directivos creados al interior de las entidades para el manejo de los recursos públicos, en áreas de tesorería, se consideran como "Cargos de Confianza". Por esto se recomienda que estos cargos se provean por personal de Libre Nombramiento y Remoción
e. Se debe realizar estudios de seguridad dentro de los procesos de contratación diseñados para proveer los cargos de tesorería, manteniendo en todos los casos, garantías de confiabilidad para la información analizada

En el Área de Tesorería:

a. Dentro de la tesorería, dependiendo de las competencias funcionales, se consideran como áreas con acceso restringido donde laboran los funcionarios y/o contratistas de la dependencia.
b. Esta área debe contar con un sistema de control de acceso con huella dactilar.
c. Los funcionarios deben poseer y portar su carné de acceso (debidamente marcado con nombre y fotografía)
d. Los visitantes deben ser autorizados por el funcionario que los va a atender, quien deberá siempre acompañarlos durante su instancia en el área. En el momento que entren a la Tesorería, deben registrarse en un libro de control describiendo la actividad a realizar.
e. Debe permanecer cerrada y asegurada los fines de semana y horas no hábiles, se deben autorizar los accesos en horarios no hábiles.
f. Se debe asegurar el área con cinta de seguridad los fines de semana y retirarse el primer día hábil de la semana, labor que realizará la compañía de seguridad y vigilancia de la entidad en compañía con un colaborador de tesorería.
g. Siempre que sea posible, la atención a visitantes debe realizarse fuera del área de tesorería.
h. Se debe contar con un punto de seguimiento y control, ejercido por la empresa de vigilancia las 24 horas.

Gestión de Cheques de Gerencia y Notas Debito

a. La solicitud de los cheques de gerencia se realiza mediante oficio dirigido a la entidad financiera, detallándose el tercero beneficiario y valor a debitar; esta comunicación debe ir firmada siempre de forma conjunta por dos personas, las cuales están previamente autorizadas y registradas en el banco.
b. Para el caso, en los que se deben utilizar este mecanismo de autorización, se debe tener en cuenta que la confirmación de las operaciones se hará únicamente por los funcionarios que la firman, o por las personas directamente vinculadas a este proceso dentro de la tesorería validando los datos tanto de la operación como los del funcionario que confirma cada operación.
c. Posteriormente, se ingresa al portal bancario, donde se hace el cargue del oficio. Los cheques son reclamados personalmente por el funcionario que designe la Tesorería.
d. Una vez los cheques son entregados en ventanilla del banco, deben ser custodiados en la caja fuerte, a cargo de un único funcionario, el cual es el encargado de revisarlos y asignar a la persona que va a realizar los pagos (pago de impuestos, AFC, pensiones voluntarias, embargos, trasferencia vía Sebra) a las diferentes entidades financieras o al Dirección de Tesoro Nacional.

Canales Electrónicos

a. La tesorería debe tener suscritos contratos con entidades financieras para la realización de pagos electrónicos. Se deben propender por rotar el pago en diferentes entidades, con el fin de garantizar transparencia y reducir el riesgo operativo.
b. Los equipos tecnológicos deben contar con herramientas de control de software malicioso activas y actualizadas.
c. En la medida que la capacidad lo permita se debe contar con un equipo exclusivo para realizar las transacciones en los portales bancarios el cual debe contar con restricciones de instalación de aplicaciones, navegación y dispositivos extraíbles (DVD, SD, USB, entre otros).
d. Se debe garantizar la continua actualización de los parches de seguridad del sistema operativo.
e. Se deben monitorear periódicamente las condiciones de seguridad de los equipos utilizados para el ingreso de transacciones.
f. Se debe contar con una clara definición de perfiles relacionados con la administración, operación y autorización de operaciones financieras.
g. La configuración de usuarios se debe realizar en relación con: estado, montos máximos, número de procesos, horarios y días de operación, productos autorizados y novedades posibles.
h. Todos los archivos usados en los procesos deben estar cifrados hasta antes de subirse a los portales bancarios con el fin de garantizar su integridad.

Seguridad en el Manejo de claves Bancarias

a. Las claves de acceso son personales y de uso exclusivo para las operaciones y transacciones que la entidad le autoriza a realizar.
b. Las claves asignadas deben ser cambiadas periódicamente por el usuario autorizado para tal fin.
c. Se debe solicitar a la entidad financiera, la asignación de algún mecanismo adicional a la clave para tener doble autenticación (ejemplo, token, tarjeta claves). Este mecanismo de autenticación asignado debe contar con protocolos de custodia y se deben tener claros los procedimientos para los casos de extravió o perdida.
d. Se deben notificar a las entidades financieras, eventos como vacaciones remplazos, encargos, cambios de cargo o cualquier situación que signifique la inactivación de cualquiera de los usuarios encargados de claves de acceso. Lo anterior, en un plazo oportuno, no mayor a 48 horas.
e. Las claves de acceso a los bancos y demás portales electrónicos deben cambiarse por lo menos cada dos (2) meses.

Conexión con las entidades Financieras

a. Solicitar a la Oficina de Tecnologías de la Información (OTI) de la Unidad que apoye a la tesorería para que esta cuente con una dirección IP exclusiva, que permita la conexión con los bancos a través de un portal o página Web.
b. Estos sitios deben estar debidamente certificados como sitios seguros de Certicamara u otro ente certificado autorizado en Colombia que tenga la facultad de expedir certificados y firmas digitales.
c. Para la conexión se recomienda implementar canales de datos dedicados, debidamente protegidos con firewall, prevención de intrusos, controles de contenido, anti-key-loggers, y antivirus entre otros, con el propósito de garantizar la seguridad en las comunicaciones y la confiabilidad de las operaciones.
d. La conexión a las entidades financieras para la realización de operaciones debe realizarse únicamente desde las direcciones IP fijas inscritas previamente en las entidades financieras.

Conexión página Ministerio de Hacienda

a. Mantener una óptima conectividad para trabajar en el Sistema Integrado de Información Financiera (SIIF). Para ello se debe tener acompañamiento permanente de la OTI, en el momento que se requiera sin necesidad de recurrir a la plataforma de incidencias y solicitudes GLPI, debido a que las tareas que se realizan en el SIIF, son de alto grado de importancia y responsabilidad.
b. La OTI debe estar atento a cualquier actualización que haya en la plataforma del SIIF para su correcto funcionamiento, o en el explorador en el que se puede acceder a este sitio, minimizando de esta manera cualquier error que pueda existir. Deben estar actualizados todos los certificados digitales con los cuales se realizan las transacciones y operaciones en el SIIF.

Carpetas Compartidas

a. Guardar los archivos de control en una carpeta compartida creada para que sea uso exclusivo de los colaboradores de la Tesorería.
b. Contar con una carpeta compartida con el Grupo de Proyectos Productivos en la cual se manejan todos los archivos en Excel y en TXT para el pago de los incentivos a las víctimas de los convenios suscritos entre la Unidad y el Banco Agrario de Colombia.
c. Contar con un software que descifre los archivos con su respectiva clave con el fin de poder cargarlos en el portal Bancario.

8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES

El acceso de los proveedores a los activos de la Unidad debe contemplar requisitos de seguridad de la información para mitigar los riesgos asociados a la confidencialidad de la información.

Lineamientos:

a. Durante la Etapa Previa[7], desde la construcción de los estudios previos (GC-FO-05), el jefe de la dependencia interesado en la contratación debe identificar los riesgos de seguridad de la información los cuales serán parte de la estimación y cobertura de los riesgos del proceso de contratación. De acuerdo con lo anterior, el análisis de riesgos de seguridad de la información debe incluir la identificación de los mismos en la respectiva contratación, su clasificación, probabilidad de ocurrencia estimada, su impacto, la determinación de la parte que debe asumirlos, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.
b. Así mismo, el Comité evaluador debe identificar sí el objeto de la propuesta u oferta evaluada, requiere del acceso de los proveedores a la información, sistemas de información y/o áreas seguras de la entidad. Independientemente del tipo de acceso que se requiera, a fin de determinar los requisitos mínimos de seguridad y los controles necesarios por parte del proveedor para ejecutar dicho contrato. En cualquiera de los casos, se debe dar a conocer a los proveedores interesados, las políticas complementarias de seguridad de la información, especialmente la Política de Uso Aceptable de los Activos y Política de Control de Acceso.
c. En medio de la Etapa Contractual, se debe asegurar la inclusión de la cláusula de confidencialidad, protección de datos, derechos de propiedad intelectual y derechos de autor, en la suscripción y perfeccionamiento del contrato que se celebre entre la entidad y aquellos proveedores que tendrán acceso a la información de la Unidad.
d. Durante la Etapa Post Contractual, es función del supervisor y/o interventoría asignada, monitorear y hacer seguimiento a los controles pactados para asegurar la confidencialidad, integridad y disponibilidad de la información, frente a los riesgos previamente identificados.
e. Antes de iniciar la ejecución del contrato, el supervisor debe socializar a los proveedores la Política para la gestión de incidentes de seguridad de la información y acordar el canal para su debido reporte.
f. Para los servicios de tecnología y de comunicaciones contratados externamente, se debe exigir que los proveedores divulguen sus requisitos y prácticas de seguridad, a lo largo de la cadena de suministro.
g. Toda gestión del proveedor que represente una modificación, mantenimiento, revisión al servicio de tecnología de la información, comunicaciones o equipos de suministros, debe pasar por el Procedimiento Gestión de Cambios, antes de su ejecución.
h. Para la contratación de servicios o componentes de la infraestructura de TI y/o áreas seguras, se debe exigir a los proveedores la presentación de los planes de continuidad de negocio que aseguren la disponibilidad de la información, suministrada y procesada entre las partes.
i. Evaluar los riesgos de la tercerización de actividades. En relación con la contratación bajo el modelo de outsourcing, tener en cuenta:
    - El acceso lógico y físico de los activos de información de la Unidad de Restitución de Tierras y los privilegios requeridos por proveedor para cumplir el contrato.
    - La sensibilidad, volumen y valor de los activos de información a los cuales van a tener acceso.
    - Los riesgos comerciales, cuando el proveedor no presta adecuadamente el servicio, o no se cumplen con los niveles de servicio pactados.
    - Los posibles conflictos de intereses que se puedan presentar.
j. Los demás lineamientos deben aplicarse de acuerdo con el Manual de Contratación (GC-MA-02) y el Manual de supervisión e interventoría (GC-MA-01) definidos por la entidad.
k. Seguir las siguientes actividades para el borrado de información si el proveedor brinda los equipos de cómputo para manejar información de la entidad:[8]

[7] *Ver Manual de Contratación (GC-MA-02)*

[8] Ver PROTOCOLO PARA EL BORRADO SEGURO DE LA INFORMACION PARA EQUIPOS ALQUILADOS SIN RECUPERACIÓN

a. Disponer del software licenciado para efectuar el borrado seguro de la información residente en los discos duros de los equipos salientes, también cuando se presenten daños de discos duros, durante el plazo de ejecución o el reemplazo de un equipo de cómputo.
b. Realizar el borrado de los discos duros, el cual debe realizarse antes de retirar los equipos de las instalaciones de la unidad, el borrado seguro debe realizarse en presencia del personal de soporte técnico de la Unidad el cual asistirá el inicio y el final del procedimiento para verificar su correcta ejecución.
c. Si se trata de un reemplazo un disco duro y se realiza migración de información, los medios utilizados para este fin también deben pasar por el mismo procedimiento de borrado.
d. Certificar el borrado de la información en el equipo a retirar, en el formato dispuesto por el CONTRATISTA.

9. EXCEPCIONES A LA PRESENTE POLÍTICA

Las excepciones requeridas por los colaboradores a la presente política deberán estar justificadas y documentadas y autorizadas por los jefes o supervisores. Estas excepciones deben ser revisadas periódicamente para garantizar su adecuado uso. Cabe anotar que estas excepciones serán recopiladas por el dominio de Seguridad de la Información.

10. DOCUMENTOS RELACIONADOS

GT-PT-05 PROTOCOLO CONFIGURACIÓN CLIENTE FORTICLIENT
GT-PT-06 PROTOCOLO PARA EL USO DEL GESTOR DE CONTRASEÑAS KEEPASS
GT-PT-07 PROTOCOLO PARA EL BORRADO SEGURO DE LA INFORMACIÓN SIN RECUPERACIÓN
GT-PT-08 PROTOCOLO GENERACIÓN COPIAS DE RESPALDO EN ESTACIONES USUARIOS
GC-MA-02 MANUAL DE CONTRATACIÓN
GT-IN-03 INSTRUCTIVO PARA COPIAS DE SEGURIDAD Y RECUPERACION EN SERVIDORES

11. CONTROL DE CAMBIOS

Se ajustan los objetivos y la estructura de gobierno y roles de seguridad de la información, se incluye en el ítem 7.2.1 El termino trabajo en casa, se vinculan al documento GT-IN-03 INSTRUCTIVO PARA COPIAS DE SEGURIDAD Y RECUPERACION EN SERVIDORES y GT-PT-09 Protocolo de Conexión y Acceso - Trabajo en Casa. Se realizan ajustes de forma al documento.

	NOMBRE:	CARGO / ROL	FECHA	FIRMA:
ELABORADO POR:	Francisco Andrés Daza Cardona	Oficial de Seguridad de la información	29/09/2020	Original Firmado
	Martin J. Puerto Ch.	Contratista OAP	29/09/2020	Original Firmado
REVISADO POR:	Claudia Patricia Hernández Díaz	Jefe Oficina Asesora de Planeación Representante de la Dirección para el SIG	29/09/2020	Original Firmado
APROBADO POR:	Enrique Cusba García	Jefe Oficina de Tecnologías de la Información.	29/09/2020	Original Firmado