1. Objetivo

Alinear, establecer y mantener un sistema de gestión de seguridad de la información que garantice la confidencialidad, integridad y disponibilidad de los datos, protegiendo la privacidad de la información tanto interna como externa, conforme a los requisitos de la norma ISO 27001. Este objetivo se orienta a mitigar riesgos, prevenir accesos no autorizados y asegurar el cumplimiento de las normativas legales y contractuales, fomentando una cultura de seguridad en toda la organización

2. Alcance

Aplica a los funcionarios, terceros, proveedores y la ciudadanía en general. Las acciones y decisiones relacionadas con el modelo de gestión de seguridad de la información se basarán en los siguientes principios:

1. **Minimizar el riesgo**
2. **Cumplir con los principios de seguridad de la información**.
3. **Cumplir con los principios de la función administrativa**
4. **Mantener la confianza**
5. **Apoyar la innovación tecnológica**
6. **Proteger los activos tecnológicos**
7. **Establecer lineamientos de seguridad**
8. **Fortalecer la cultura de seguridad**
9. **Garantizar la continuidad del negocio**

3. Responsables

- Jefe Oficina Estratégica
- Profesional Especializado de la oficina estratégica
- Profesional Universitario Grado 1 y 2 Oficina Estratégica TI
- Técnico Administrativo Grado 1 y 2 Oficina Estratégica TI

Será responsabilidad de este equipo velar por el mejoramiento continuo de las distintas actividades que se realizarán enfocadas a la seguridad de la información, verificación del avance de los distintos proyectos, la revisión del documento de la política de seguridad y privacidad de la información y la verificación del cumplimiento de las políticas.

4. Terminos y Definiciones

- **Listas negras:** son herramientas de seguridad utilizadas para identificar y bloquear el acceso a ciertos elementos considerados indeseables o peligrosos. Estas listas pueden incluir direcciones IP, dominios, correos electrónicos o software malicioso que se ha asociado con actividades fraudulentas, spam o ataques cibernéticos.
- **Sistema internos:** son aquellos sistemas, aplicaciones y procesos que están diseñados y operan dentro de una organización. Estos sistemas son utilizados para gestionar y facilitar las operaciones, la comunicación y la toma de decisiones internas. Los sistemas internos de la ESU son:

1. Infraestructura de TI
2. Procesos operativos
3. Seguridad de la información
4. Aplicativos en la nube: Esuguard, Datascrum, Parque automotor, Portal de contratación.

- **Sistemas externos:** se refieren a aquellos sistemas o aplicaciones que operan fuera del entorno de una organización, pero que pueden interactuar con sus procesos, datos o infraestructura. Los sistemas externos de la ESU son:

- Safix
- Hyperbpm

- Número MAC: es una dirección única asignada a la interfaz de red de un dispositivo para identificarlo en una red.

5. Aprovisionamiento de equipos

Realizar seguimiento y control anualmente al licenciamiento del software y aplicaciones de la Entidad. El proceso de Gestión de la Tecnología de la Información definirá el software y aplicaciones que se encuentran permitidas para ser instaladas en las áreas de la entidad son las siguientes:

- Foxit Reader
- Google chrome
- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Java 8 Update 301
- Microsoft Office365
- 7-zip
- Microsoft OneDrive
- VPN Forticlient

Esta base está definida y aprobada, en caso de requerir software adicional el proceso de Gestión de la Tecnología de la Información será el único encargado de evaluarlo y aprobarlo.

Gestión de medios removibles

- Autorizar, ejecutar y monitorear el uso de medios removibles (CDs, USBs, discos duros, Smartphone, memoria Flash, MP3 y demás dispositivos tecnológicos) a funcionarios, practicantes y/o contratistas que cuenten con autorización previa del Jefe Oficina, Subgerente de área, Secretario General y Gerente. Estos deberán aceptar por escrito los riesgos de seguridad a los que están expuestos.
- Garantizar que los puertos físicos y lógicos de diagnóstico y configuración de los equipos que soportan los sistemas de información siempre estén restringidos y monitoreados con el fin de prevenir accesos no autorizados.
- Asegurar física y lógicamente los diferentes accesos a la red corporativa, con el fin de no poner en riesgo la seguridad de la información mediante cualquier dispositivo extraíble.

6. Disposición de la Información

- **Copias de Seguridad**: El área de Gestión de la Tecnología de la Información (GTI) tiene la responsabilidad de realizar copias de seguridad (backups) de todos los activos que manejen, almacenen, procesen y ejecuten información corporativa. Esto se llevará a cabo durante actividades como retiro, traslado, reasignación o remate, garantizando el resguardo y recuperación de la información.
- **Autorización de Copias de Seguridad**: La GTI es la única autoridad para autorizar la realización de copias de seguridad de la información. Esto es fundamental para evitar la pérdida o el borrado no autorizado de datos.
- **Responsabilidades de los funcionarios y contratistas**: Todos los funcionarios y contratistas de la entidad son responsables de gestionar y proteger los activos de información a su cargo o a los que tengan acceso. Esto asegura que se mantengan los niveles de seguridad durante todo el ciclo de vida de la información.
- **Instalación de Software y Hardware**: El área de Tecnología de la Información es la única autorizada para instalar cualquier tipo de software o hardware en la entidad. Sin embargo, esta área no tiene permitido manipular la información generada dentro de los procesos.
- **Notificación de Retiro de Activos Tecnológicos**: Se debe notificar a Gestión de la Tecnología de la Información (GTI) mediante el procedimiento establecido al retirar un activo tecnológico de la entidad. La notificación debe incluir:

1. Fecha y hora del retiro
2. Tiempo que el activo estará fuera de las instalaciones
3. Lugar donde se encontrará el activo

Esta información será corroborada por el jefe de cada área correspondiente.

6.1 Protección de Equipos

Todos los funcionarios y contratistas deben proteger adecuadamente los equipos de la infraestructura tecnológica para prevenir:

- Pérdida
- Daño
- Robo
- Accesos no autorizados

- **Ubicación de Equipos**

Los equipos deben ser ubicados lejos de áreas con amenazas potenciales, tales como:

- Fuego
- Explosivos
- Agua
- Polvo
- Vibraciones
- Interferencia electromagnética
- Vandalismo

- **Comportamiento en Áreas Tecnológicas**

Se debe evitar fumar, beber o consumir alimentos cerca de los equipos de la infraestructura tecnológica de la entidad.

- **Reubicación de Equipos de Cómputo**

Los equipos de cómputo fijos asignados a funcionarios y contratistas solo podrán ser reubicados por el área de Gestión de Tecnología de la Información.

Asimismo, el personal que salga de vacaciones o tenga una incapacidad superior a ocho días deberá realizar la entrega del equipo asignado al personal de TI de la organización, con el fin de permitir la realización de actualizaciones correspondientes y garantizar la seguridad de la información.

6.2 Dispositivos móviles

- Conectar a la red inalámbrica corporativa de la Entidad únicamente los equipos de cómputo asignados a los funcionarios y/o contratistas desde el proceso de Gestión de Tecnología de la Información, por consiguiente, está prohibido conectar cualquier dispositivo móvil a la red.
- El área de TI permitirá la conexión de dispositivos móviles a la red inalámbrica de invitados exclusivamente a terceros que así lo requieran, que cuenten con autorización previa del Jefe Oficina, Subgerente de área, Secretario General y Gerente.

Estos deberán aceptar por escrito los riesgos de seguridad a los que están expuestos.

- Todos los dispositivos móviles deberán instalar y ejecutar la aplicación Microsoft Authenticator para proteger la información de los funcionarios que deseen agregar y sincronizar su cuenta de correo electrónico.
- Los funcionarios, practicantes y/o contratistas que cuenten con dispositivos móviles corporativos, están obligados almacenar, usar y compartir exclusivamente información relacionada al cargo.
- El proceso de TI prohíbe el uso de aplicaciones que no sean coherentes con los procesos internos de la entidad, a los diferentes dispositivos que hagan parte de sus activos.
- Los mensajes y la información contenida en las cuentas de correo son propiedad de la Entidad, cada usuario es responsable de su buzón, y deberá mantener solamente información relacionada con el desarrollo de sus funciones. Las conversaciones por el chat corporativo Teams con funcionarios y/o terceros ajenos a la entidad, solo están permitidos para el desarrollo de las funciones propias del cargo.
- No está permitido intercambiar información no autorizada desde cualquier medio de comunicación que sea de propiedad de la ESU, con terceros ajenos a la organización.

7. Seguridad De La Información En Las Redes Corporativas

Control de redes corporativas:

- El proceso de Gestión de Tecnología de la Información tendrá la potestad de realizar las configuraciones necesarias a nivel de firewall para controlar las descargas de archivos de acuerdo con los criterios de seguridad para garantizar la seguridad de la red e información de la entidad.
- El proceso de Gestión de Tecnología de la Información serán los responsables de crear y configurar las reglas y restricciones necesarias a nivel de firewall para cada usuario de acuerdo a los perfiles laborales, para controlar el acceso, descargas y consumo no autorizados.
- Separar la red en segmentos físicos y lógicos para independizar la red de usuarios de conexión con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. El proceso de Gestión de la Tecnología de la Información es el encargado de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
- Establecer mecanismos de identificación automática de los equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la Entidad.

- Se debe garantizar que los puertos físicos y lógicos de diagnóstico y configuración de los equipos que soportan los sistemas de información estén siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.
- Se prohíbe a los funcionarios y/o terceros conectar cualquier equipo a la red LAN o WLAN que no pertenezca al dominio esu.com.co. Solo se permite la conexión de equipos que hayan sido previamente autorizados por el proceso de TI.

8. Correo electrónico Y Herramientas De Colaboración Del Office 365
Políticas de uso:

- Usar la cuenta de correo electrónico asignada únicamente para el desempeño de las funciones dentro de la entidad.
- Todas las cuentas de correo deben configurarse con autenticación de doble factor.
- Solo se podrán enviar y/o recibir correos electrónicos que tengas un peso máximo de 25 Mb.
- Para enviar mensajes publicitarios corporativos el proceso de Gestión de Tecnología de la Información es el autorizado para aprobar la solicitud presentada por el proceso de Gestión de la Comunicación, con el fin de evitar posibles bloqueos o inclusiones en listas negras.
- Todos los Grupos de distribución serán creados y configurados por el proceso de Gestión de la Tecnología de la Información, previa solicitud del proceso de Comunicaciones.
- No está permitido enviar cadenas de correo, ni mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo, o cualquier otro tipo de mensajes que atenten contra la dignidad o la productividad de las personas, así como el normal desempeño del servicio de correo electrónico de la entidad que afecten los sistemas internos o de terceros, aquellos que vayan en contra de las leyes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Está prohibido enviar y/o recibir archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por el proceso de Gestión de Tecnología de la Información.
- No está permitido abrir correos clasificados como maliciosos o peligrosos que contengan virus o malware que ponga en riesgo la seguridad de la información.
- Toda información de la ESU generada con los diferentes programas computacionales (Ej. Office, Shopos, Acces, Etc.) que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.
- Está prohibido usar la dirección de correo electrónico de la ESU como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, Twitter, Instagram o cualquier otro sitio que no tenga que ver con las actividades laborales.
- El proceso de Gestión de la Tecnología de la Información tendrá la potestad de bloquear y generar una lista negra de correo electrónico de remitentes que considera potencialmente peligroso.

9. Control de Acceso
Control de acceso con usuario y contraseña:

- El proceso de Gestión de la Tecnología de la información tendrá la potestad de implementar cualquier tipo de autenticación a los sistemas de información, tales como (Radius 802.1x, Ldap, entre otros)
- Todo funcionario, practicante, y/o contratista que requiera acceso a los sistemas de información de la ESU debe contar con un usuario y contraseña asignado por el proceso de Gestión de la Tecnología de la Información, previamente solicitado por la Unidad de Gestión humana.
- Todo funcionario, practicante y/o contratista contará con un usuario compuesto por la letra inicial del primer nombre y el primer apellido completo, con el fin de permitir el acceso a los diferentes aplicativos y herramientas corporativas.
- Los usuarios de terceros o contratistas tendrán las mismas políticas que los usuarios de planta, adicionando la extensión .ext en el login de usuario.
- Los usuarios practicantes tendrán las mismas políticas que los usuarios de planta, creando de manera general el login de usuario, tales como (pghumana, pfinanciera, pservicios, pcompras, pdocumental, entre otros continuando con las mismas siglas)
- El área técnica de la Gestión de Tecnología de la información es la única persona autorizada para crear, modificar, suspender y/o eliminar usuarios de la red de acuerdo a las directrices avaladas y debidamente documentadas desde el proceso de Gestión Humana o jefe inmediato y eventos relacionados que así lo requieran.
- Las contraseñas de acceso a los diferentes sistemas de información no deben compartirse con otros funcionarios. Hacerlo expone al usuario a consecuencias disciplinarias y/o judiciales por las acciones que otras personas realicen con la misma. Es responsabilidad del usuario el uso inadecuado de sus credenciales de acceso.
- El proceso de Gestión Humana será el único canal autorizado para solicitar la creación, suspensión, y/o eliminación de un usuario de los sistemas de información de la entidad.
- El proceso de Gestión de Tecnología de la Información establecerá y clasificará los permisos de acceso de cada usuario a los sistemas de información de acuerdo con las funciones asociadas al cargo.

9.1 Inventario de activos de la información

- Servidor directorio activo
- Servidor respaldo de información ZEUS
- Servidor sistema biométrico Workstation
- Aplicativos en la nube

9.2 Creación y/o modificación de usuarios para los módulos de SAFIX:

- Previa solicitud de las diferentes áreas de la entidad y bajo autorización del jefe inmediato, se realizará la creación y/o modificación de usuarios en los diferentes módulos del sistema acorde a las necesidades y tareas del funcionario.
- La solicitud se debe realizar por el Jefe inmediato en la mesa de ayuda del área de tecnología de la información, especificando claramente, los permisos y restricciones según el rol a desempeñar dentro del sistema de información.
- Los roles podrán ser creados por módulo y asignar acceso a las diferentes formas que requieran.
- Se podrán crear usuarios de administración, de consulta

9.3 Gestión de la información

La información y los datos de la organización deben ser clasificada en alguno de los siguientes niveles, teniendo en cuenta su nivel de confidencialidad dentro de la operación de la ESU:
Confidencial: cuando el nivel de confidencialidad de la información se incremente
Restringido: para niveles medios de confidencialidad
Uso interno: información con un nivel bajo de confidencialidad
Público: cuando todas las personas pueden ver la información

10. Seguimiento del Control de acceso

El responsable de la operación de la Gestión de Tecnología de la Información será el único autorizado para utilizar un usuario con privilegios superiores, y será responsable exclusivo de la administración de cualquier sistema de información, aplicación, base de datos y/o herramienta de la entidad.

El proceso de Gestión de Tecnología de la Información será el encargado de crear, modificar o revocar, cuando sea necesario, los privilegios de uso o acceso a las aplicaciones, herramientas o sistemas de información, asignados a los usuarios (ID) creados en la red corporativa.

- Está estrictamente prohibido que cualquier funcionario o tercero de la entidad utilice, administre o ejecute un usuario (ID) con privilegios superiores sin previa autorización del proceso de Gestión de Tecnología de la Información.
- **Acceso físico:** El acceso al Datacenter estará restringido mediante controles de seguridad biométrica y una cerradura interna de seguridad, bajo la exclusiva responsabilidad del personal de TI.
- **Doble factor de autentificación:** Se utiliza un software de autenticación de Microsoft, conocido como **Authenticator**, para gestionar el inicio de sesión en todos los aplicativos de Office 365. Este mecanismo es empleado tanto para el acceso al correo electrónico como para la intranet, garantizando un proceso seguro y centralizado de autenticación para los usuarios.
- **Acceso lógico:**
  - Contraseñas robustas de un mínimo de 12 caracteres.
  - Implementación de doble autenticación como medida de seguridad adicional.
  - Los administradores de TI dispondrán de cuentas con privilegios de superusuarios.
  - Los usuarios tendrán permisos asignados únicamente de acuerdo con el rol correspondiente.

Actualmente, existen reglas definidas para la gestión del acceso físico y lógico a la información y a los activos asociados, en cumplimiento con los requisitos de seguridad de la información del negocio.

10.1 Gestión de Contraseñas

Para garantizar la seguridad en el acceso a la red corporativa y a los sistemas de información, se deben considerar los siguientes aspectos al momento de crear contraseñas:

1. **Longitud y complejidad:**
   - Mediante el proceso de Hardening, se ha configurado la autenticación para aceptar contraseñas con una longitud mínima de 16 caracteres y máxima de 22.
   - La contraseña debe incluir al menos ocho (8) caracteres alfanuméricos.
2. **Sincronización de contraseñas:**

- La contraseña de acceso a la red corporativa estará sincronizada con la cuenta de correo electrónico del usuario.

3. **Historial de contraseñas:**

   - No se permite reutilizar ninguna de las últimas seis (6) contraseñas asignadas al usuario.

4. **Caducidad y actualización:**

   - Las contraseñas tendrán una vigencia de un (1) mes.
   - El sistema enviará una notificación de advertencia antes de la caducidad para que el usuario pueda realizar la actualización correspondiente.

5. **Restricciones en el contenido de la contraseña:**

   - Está prohibido utilizar datos personales, nombres de familiares o cualquier palabra relacionada con información personal en la contraseña.
   - No se permite el uso de combinaciones simples o fácilmente adivinables, como "Abcd1234", nombres de meses, años u otras variantes similares.

6. **Intentos fallidos y bloqueo:**

   - Si un usuario introduce la contraseña incorrectamente más de cinco (5) veces, la cuenta será bloqueada automáticamente.
   - El desbloqueo únicamente podrá ser realizado por el administrador de la operación de la Gestión de Tecnología de la Información.

10.2 Perímetros de Seguridad

El proceso de Gestión de Tecnología de la Información será el encargado de definir los roles y responsabilidades relacionados con el nivel de acceso y privilegios asignados a los funcionarios que interactúan con la infraestructura tecnológica y los sistemas de información de la empresa. Este enfoque busca reducir y evitar el uso no autorizado o la modificación de los activos de información de la entidad.

Control de Acceso y Protección de Activos

1. **Control de acceso físico:**

   - Se establecerán medidas de control de acceso físico en el perímetro de las áreas destinadas al procesamiento o almacenamiento de información sensible.
   - Estas medidas serán auditables y estarán diseñadas para proteger la información, el software y el hardware de daños intencionales o accidentales.
   - Incluye la protección de las áreas que albergan equipos e infraestructura de soporte para los sistemas de información y comunicaciones.

2. **Acceso remoto y cifrado de datos:**

   - Todas las conexiones remotas a la infraestructura tecnológica estarán protegidas mediante cifrado de datos.
   - Los accesos remotos serán gestionados por el proceso de Gestión de Tecnología de la Información, de acuerdo con las necesidades específicas de cada usuario y previa autorización del Subgerente de área correspondiente.
   - Cada usuario será responsable de garantizar la seguridad, confidencialidad e integridad de la información a la que accede de forma remota.

3. **Monitoreo y acceso al centro de datos:**

   - Se implementarán reglas de monitoreo y control de acceso al centro de datos.
   - Solo el personal autorizado por el proceso de Gestión de Tecnología de la Información podrá acceder al software y hardware de los sistemas de información, mitigando riesgos de daños o accidentes en la infraestructura tecnológica.

Gestión de Accesos y Separación de Roles

- El administrador de tecnología implementará reglas estrictas de acceso para los sistemas críticos y medianamente críticos de la entidad.
- Las personas que administran, operan, mantienen, auditan o acceden a estos sistemas tendrán roles separados, asegurando una clara segregación de funciones.
- Los permisos de acceso serán otorgados por un responsable distinto al que los utiliza, fortaleciendo la seguridad y reduciendo riesgos de errores o abusos.

11. Protección Permanente Contra Software Malicioso

La entidad se compromete a proteger todos sus recursos informáticos mediante el uso de herramientas y software de seguridad, tales como antivirus, anti-spam, antispyware y otras aplicaciones diseñadas para prevenir y combatir la entrada de código malicioso en la red.

Medidas de Protección

1. **Uso de herramientas de seguridad:**
    - Actualmente, la entidad cuenta con antivirus actualizados, adecuados para detectar y prevenir posibles fallos causados por código malicioso.
    - El proceso de Gestión de Tecnología de la Información será responsable de autorizar el uso de estas herramientas, garantizar su actualización permanente y asegurar que no sean deshabilitadas bajo ninguna circunstancia.
2. **Análisis y desinfección de dispositivos:**
    - Se debe realizar un análisis de seguridad y desinfección mediante el antivirus a todos los dispositivos de almacenamiento que se conecten a los equipos de la entidad.
3. **EDR (Endpoint Detection and Response):**
    - La entidad utiliza EDR (detección y respuesta en el punto final), una herramienta avanzada de ciberseguridad que permite detectar, investigar y responder a amenazas en dispositivos finales, como ordenadores, portátiles y servidores.
    - Los puntos finales son considerados objetivos potenciales de ciberataques debido a su contacto con información sensible, por lo que están bajo estricta supervisión de seguridad.
4. **Restricciones sobre puertos USB:**
    - Bajo ninguna circunstancia se activarán los puertos USB de los equipos sin autorización escrita del jefe inmediato.

Prohibiciones

Para garantizar la seguridad de la infraestructura tecnológica, está estrictamente prohibido:

- Desinstalar o desactivar el software y/o herramientas de seguridad previamente avaladas por la entidad.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código diseñado para replicarse automáticamente, dañar o afectar el desempeño de dispositivos o la infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.
- Usar código móvil no autorizado previamente por el proceso de Gestión de Tecnología de la Información.

Estas directrices refuerzan el compromiso de la entidad con la protección de su infraestructura tecnológica y la prevención de ciberataques, asegurando la integridad, confidencialidad y disponibilidad de sus recursos informáticos.

12. Acceso a Internet

Uso Adecuado de los Recursos

Es responsabilidad de los usuarios dar un uso adecuado a los recursos de la red corporativa, evitando prácticas ilícitas o malintencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información.

Control y Monitoreo de Navegación

1. **Supervisión del uso de internet:**
    - Se controlará, verificará y monitoreará de manera permanente la información, el uso y la navegación en internet de todos los usuarios, incluidos funcionarios, invitados y terceros que se conecten a la red de la entidad.
    - Este monitoreo tiene como objetivo garantizar el uso eficiente del canal corporativo y mantener la seguridad de la información.
2. **Monitoreo detallado:**
    - Se realizará un monitoreo continuo de los tiempos de navegación, páginas visitadas y el consumo de ancho de banda por parte de funcionarios y/o terceros.
    - También se inspeccionarán, registrarán y evaluarán las actividades realizadas durante la navegación, cumpliendo con la legislación nacional vigente.

Restricciones en el Uso de Servicios Interactivos

- Queda restringido el acceso y uso de servicios interactivos o de mensajería instantánea como Facebook, Instagram, Yahoo, Outlook, Skype y otros similares, salvo que sean requeridos para actividades propias del negocio de la entidad.

Prohibiciones

Para garantizar la integridad de los recursos tecnológicos, está estrictamente prohibido:

1. **Acceso a contenido inapropiado:**
    - Visitar páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y cualquier otro sitio que atente contra la ética, las leyes vigentes o las políticas de la entidad.
2. **Asunción de posiciones personales en nombre de la entidad:**
    - Participar en encuestas de opinión, foros u otros medios similares asumiendo posiciones personales en nombre de la ESU, ya sea por parte de funcionarios o terceros.
3. **Descarga de contenidos no autorizados:**
    - Descargar, instalar, compartir o utilizar información audiovisual desde sitios públicos en internet sin autorización explícita del proceso de Gestión de Tecnología de la Información.
    - Para estas acciones, se debe contar con los procedimientos y controles necesarios para su monitoreo y aseguramiento.
4. **Uso de software y contenidos no autorizados:**
    - Descargar, usar, intercambiar o instalar juegos, música, películas, protectores de pantalla, software de libre distribución, archivos ejecutables, información o productos que vulneren la propiedad intelectual.
    - Emplear herramientas que comprometan la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica de la entidad.

13. Uso Eficiente De La Telefonía

Seguimiento y Control del Consumo Telefónico
El servicio telefónico institucional estará sujeto a un seguimiento y control riguroso, realizado de forma mensual, para monitorear el consumo desde las distintas extensiones habilitadas. Este servicio debe ser utilizado exclusivamente para asuntos institucionales, respetando los principios de racionalidad y austeridad del gasto público.

Lineamientos de Uso

1. **Acceso y restricción de llamadas:**
    - Las llamadas salientes y entrantes no tendrán restricciones de tiempo para ningún usuario.
    - Solo se permite la realización de llamadas locales desde las extensiones habilitadas para los usuarios de la entidad.
2. **Llamadas locales:**
    - Todas las extensiones estarán habilitadas para realizar llamadas locales.

14. Privacidad Y Confidencialidad

La privacidad y confidencialidad de la ESU se encuentra regulada mediante la **Política de Protección de Datos Personales**, la cual está disponible para consulta pública en la página web oficial de la entidad, a través del siguiente enlace: Política de Protección de Datos Personales.

Este documento puede ser consultado por los funcionarios y la ciudadanía en general para garantizar la transparencia y cumplimiento de las disposiciones legales relacionadas con la protección de datos personales.

15. Integridad

Todo funcionario, practicante y/o contratista deberá incluir en su firma oficial de correo electrónico el siguiente mensaje, que asegura el cumplimiento de la integridad y confidencialidad de la información:

“La información contenida en este correo electrónico es confidencial y solo puede ser utilizada por el destinatario autorizado, ya sea un individuo o una compañía. Si usted no es el destinatario autorizado, queda prohibida su retención, difusión, distribución o copia, según lo establecido por la ley. Si ha recibido este mensaje por error, le ofrecemos disculpas y le solicitamos eliminar inmediatamente el mensaje y sus adjuntos.”

Además, todas las firmas oficiales incluirán automáticamente un mensaje en la parte inferior que indicará:
“Este mensaje es confidencial.”

15.1 Intercambio Seguro De Información

Todo funcionario, practicante y/o contratista tiene la responsabilidad y la obligatoriedad de cumplir con las políticas y procedimientos establecidos para garantizar la integridad y el intercambio seguro de la información. Para ello, se deben considerar los siguientes aspectos:

1. **Protección de la Confidencialidad e Integridad de la Información**
    - Salvaguardar la información, especialmente durante su intercambio a través de diferentes medios, para prevenir su divulgación o modificación no autorizada.
2. **Acuerdos de Confidencialidad**
    - Firmar acuerdos de confidencialidad con funcionarios, clientes, proveedores y/o terceros que, por distintas razones, necesiten conocer o intercambiar información restringida o confidencial de la entidad.
    - Estos acuerdos deben especificar claramente las responsabilidades de todas las partes para garantizar un intercambio seguro y deben firmarse antes de acceder o utilizar dicha información.
3. **Definición y Cumplimiento de Requisitos de Seguridad de la Información**
    - Garantizar la definición y cumplimiento de los requisitos de seguridad de la información en coordinación con la Secretaría General.
    - Estos requisitos deberán ser incorporados en las obligaciones contractuales específicas de cada caso.

15.2 Seguridad De La Informacion En La Contratación

- **Identificación de Riesgos**

- Identificar los riesgos asociados al acceso, procesamiento, comunicación o gestión de la información y/o de la infraestructura para su procesamiento, por parte de personas o entidades externas, terceros y/o contratistas.
- Establecer mecanismos de control efectivos para garantizar que la seguridad de la información se mantenga en todo momento.

- **Cláusula de Confidencialidad**

  - Incluir una cláusula de confidencialidad de la información como parte integral de los contratos de trabajo con personas o entidades externas, terceros y/o contratistas, siempre que estos necesiten acceder a información o recursos de la Entidad.
  - La cláusula deberá garantizar lo siguiente:
    - Prohibición de divulgar, usar o explotar la información confidencial a la que tengan acceso.
    - Respeto por los niveles establecidos de clasificación de la información.
    - Aclaración de que cualquier incumplimiento de lo establecido será considerado un **"incidente de seguridad"**.

- **Contratos con Proveedores y Clientes**

  - Asegurar que en los contratos firmados con proveedores y clientes se incluya una cláusula de confidencialidad que garantice la protección y salvaguarda de la información compartida.

16. Seguridad Permanente Del Usuario

Con el objetivo de garantizar la seguridad de la información restringida o confidencial, se deben cumplir las siguientes directrices:

1. **Almacenamiento Seguro de la Información**

   - Mantener documentos impresos, CDs, dispositivos USB y medios removibles bajo llave o protegidos con contraseña en todo momento, especialmente cuando:
     - El puesto de trabajo esté desatendido.
     - Fuera del horario laboral.
   - Estas medidas evitan pérdidas, daños o accesos no autorizados a la información.

2. **Gestión de Información Impresa**

   - Recoger de manera inmediata la información sensible enviada a las impresoras para prevenir accesos no autorizados.

3. **Bloqueo de Equipos de Cómputo**

   - Bloquear la sesión del equipo de cómputo cada vez que se abandone el puesto de trabajo.
   - La sesión solo podrá desbloquearse utilizando la contraseña del usuario.
   - Al finalizar las actividades, cerrar todas las aplicaciones y desconectar la sesión de trabajo para evitar accesos indebidos.

4. **Almacenamiento en Unidades de Red**

   - Es responsabilidad del usuario final mantener la información sensible de la entidad almacenada exclusivamente en las unidades de red designadas por el proceso de Gestión de la Tecnología de la Información.

5. **Doble Factor de Autenticación**

   - Utilizar el doble factor de autenticación proporcionado por Microsoft, el cual envía un token al dispositivo móvil registrado, para garantizar un acceso seguro.

17. Registro

Desde el proceso de **Gestión de Tecnologías de la Información**, se realizan monitoreos diarios de los servicios internos de la Infraestructura Tecnológica mediante un **script en DOS**. Este script evalúa los siguientes componentes:

- Comunicación de los servidores.

- Cámaras de seguridad.
- Impresoras.
- Páginas de la entidad.
- Planta telefónica.
- Red Wi-Fi.

17.1 Almacenamiento de registros

El proceso de **Gestión de la Tecnología de la Información** establece un procedimiento para el almacenamiento de copias de seguridad de los sistemas de información, basado en metodologías reconocidas y en cumplimiento con las normativas aplicables.

1. **Responsabilidades del Área de TI**
    - Garantizar que el proveedor de servicios informáticos realice las copias de seguridad de manera periódica, conforme a la **política específica de copias de seguridad** derivada del control 8.13 de la norma **ISO 27001**.
    - Elaborar un acta a través de la herramienta Hyper como constancia de la entrega de dispositivos de backup al centro documental para su custodia segura.
2. **Eliminación de Información Irrelevante**
    - Eliminar de los servidores toda información que no esté relacionada con la ejecución de los procesos de la entidad, asegurando la optimización del almacenamiento y la protección de datos relevantes.

17.2 Garantía de Cumplimiento

Se llevará a cabo una revisión periódica de las políticas de TI con el objetivo de:

- Garantizar su **cumplimiento**.
- Asegurar su **actualización** constante.
- Facilitar su **gestión oportuna**.

18. Gestión De Incidentes De Seguridad De La Información

El equipo de trabajo de TI garantizará el **control, análisis y solución de incidentes**, así como la atención a eventos y vulnerabilidades en los sistemas de información. Esto tiene como objetivo asegurar la **disponibilidad y calidad del servicio**, mitigando riesgos asociados.

Reporte de Solicitudes e Incidentes

Los funcionarios, practicantes y/o contratistas deberán:

- Reportar cualquier solicitud, incidente, incumplimiento o infracción que ponga en riesgo la seguridad de la información.
- Utilizar los canales oficiales:
    - **Mesa de servicios**.
    - **Correo electrónico**.
    - **Llamadas telefónicas**.

Documentación:
HyperBPM

Requerimiento	ANS – Atención de solicitud.	Observación
Creación, suspensión, activación y/o desactivación de usuarios.	5 días Hábiles	Aplica desde el momento que el proceso de Gestión de Talento Humano realiza la solicitud a través de la mesa de servicios.
Configuración de rutas	2 días Hábiles	Inicia una vez reportado el requerimiento en mesa de servicios.

Permisos para consultas de documentos, expedientes y/o similares.	2 días Hábiles	Inicia una vez reportado el requerimiento en mesa de servicios.
Consultar y/o exportar información desde la Safix y consultas en SQL	2 días Hábiles	Inicia una vez reportado el requerimiento en mesa de servicios.
Servidor de aplicación caído y/o error funcionalidad que imposibilite el acceso al servicio.	1 hora Hábil	Inmediatamente se evidencia afectación en el servicio.
Incidentes a nivel de software y hardware en dispositivos y/o equipos relacionados con el proceso de Gestión Documental.	1 dia hábil	Inicia una vez reportado el requerimiento en mesa de servicios y depende de la complejidad de la solución requerida.
Requerimientos generales que tengan bajo impacto en las actividades asociadas al proceso de Gestión Documental	1 dia hábil	Inicia una vez reportado el requerimiento en mesa de servicios.

- Nota: Si el soporte se debe escalar al proveedor del software se tomarán los ANS establecidos en el contrato con el mismo.

SAFIX:

Requerimiento	ANS – Atención de solicitud.	Observación
Creación, suspensión, activación y/o desactivación de usuarios.	5 días Hábiles	Aplica desde el momento que el proceso de Gestión de Talento Humano realiza la solicitud a través de la mesa de servicios.
Asignación y/o modificación de permisos a nivel de acceso, formas y módulos.	1 días Hábiles	Inicia una vez reportado el requerimiento
Corrección de funcionalidad, proceso y errores a nivel de aplicación de alto impacto.	2 horas Hábiles	Inicia una vez reportado el requerimiento en mesa de servicios.
Corrección de funcionalidad, proceso y errores a nivel de aplicación de bajo impacto.	4 día hábil	Inicia una vez reportado el requerimiento en mesa de servicios.

- Nota: Si el soporte se debe escalar al proveedor del software se tomarán los ANS establecidos en el contrato con el mismo.

SEGURIDAD (Firewall y antivirus)

Requerimiento	ANS – Atención de solicitud.	Observación
Acceso página web.	8 horas Hábiles	Inicia una vez reportado el requerimiento en mesa de servicios y sea aprobado por el proceso de Gestión de la Tecnología.
Creación y configuración de políticas de seguridad.	8 horas Hábiles	Inicia una vez reportado el requerimiento en mesa de servicios y sea aprobado por el proceso de Gestión de la Tecnología.
Requerimientos generales de alto impacto	1-2 hora Hábil	Inicia una vez reportado el requerimiento en mesa de servicios y sea aprobado por el proceso de Gestión de la Tecnología.
Requerimientos generales de bajo impacto	1-2 día Hábiles	Inicia una vez reportado el requerimiento en mesa de servicios y sea aprobado por el proceso de Gestión de la Tecnología.
Acceso a recursos de antivirus.	6 horas Hábiles	Inicia una vez reportado el requerimiento en mesa de servicios y sea aprobado por el proceso de Gestión de la Tecnología.

REQUERIMIENTOS GENERALES

Requerimiento	**ANS – Atención de solicitud.**	**Observación**
Acceso a ruta o carpeta compartida (Servidor de archivos)	6 horas Hábiles	Inicia una vez reportado el requerimiento en mesa de servicios y sea aprobado por el propietario de la información (Si aplica)
Instalación de software	2 días Hábiles	Inicia una vez reportado el requerimiento en mesa de servicios.
Actualización de información portal de contratación de alto impacto	1 Hora	Inicia una vez reportado el requerimiento en mesa de servicios.
Actualización de información portal de contratación de bajo impacto	8 horas Hábiles	Inicia una vez reportado por el proveedor.
Error a nivel de software	8 horas Hábiles	Inicia una vez reportado por el proveedor.
Daño a nivel de hardware	2 horas Hábiles	Inmediatamente se evidencia errores en el dispositivo.
Acceso grabaciones cámaras	2 días Hábiles	Inicia una vez reportado por el proveedor y autorizado por jefe de oficina estratégica.
Requerimientos generales que afecten las actividades laborales e impidan el uso de un servicio	2 horas Hábiles	Aplica una vez reportado el requerimiento en la mesa de servicios.
Requerimientos generales que sean solicitados y generen un bajo impacto en el uso del servicio	2 día Hábiles	Inicia una vez reportado por el proveedor.

Descripción del equipo que manejará los incidentes:

- Técnico Administrativo tendrá la responsabilidad de atención y solución de requerimientos de primer y segundo nivel, manejo de proveedores si así lo requiera y quien estará a cargo de apoyar toda la operación y administración de los sistemas de información.
- Profesional Universitario de la Gestión de Tecnología de la Información tendrá la potestad de liderar y generar estrategias para las soluciones y mejoras de requerimientos que permitan mejorar los procesos de la Infraestructura Tecnológica, además de operar y administrar los sistemas de información.

CONTROL DE CAMBIOS

Versión	Fecha	Usuario	Comentario
2	14/08/2019	Marcela Salazar Valencia	Actualización según modelo actual de la Infraestructura tecnológica.
3	17/11/2021	Marcela Salazar Valencia	Se incluyó el reconocimiento a las entidades del gobierno Nacional de la seguridad de la información.
4	12/08/2022	Carlos Alberto Arcila Ospina	Se hacen cambios en las politica de acuerdo a la nueva infraestructura, cambio de aplicativos ofimáticos, sitema documental y cambio de responsables.

5	31/12/2024	Valeria Mejia	Se alinea la política con la Norma Iso 27001, estableciendo los controles de la norma
6	23/08/2025	Valeria Mejia	Debido a la actualización del Mapa de Procesos, se modifica el nombre del proceso, pasando de "Tecnología de la información" a "Gestión de sistemas de la información", lo que implica la actualización del código documental correspondiente. Se aprueba la política en el comité institucional de gestión y desempeño del 20 de agosto de 2025

ELABORÓ	REVISÓ	APROBÓ
Profesional Universitario Grado 2 - TI **Fecha de elaboración:** 01/08/2025	Profesional Especializado - Oficina Estrategica **Fecha de revisión:** 15/08/2025	Jefe de Oficina Estrategica **Fecha de aprobación:** 23/08/2025