ALCALDÍA MAYOR
DE BOGOTÁ D.C.
DESARROLLO ECONÓMICO
Instituto para la Economía Socia

IPES

MANUAL DEL SISTEMA DE GESTIÓN Y POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO

Bogotá 2024

Elaboró:	Revisó:	Aprobó:
Martha Mateus - Contratista Daniel Fragoso -Profesional Cristian Casallas - Contratista Michael Pinilla - Contratista Richard Rojas - Contratista Jairo Remolina - Contratista	Edgar Mauricio Mera Profesional Especializado Contratista - SDAE	Paola Rico Parada Subdirectora Diseño y Análisis Estratégico

TABLA DE CONTENIDO

1. OBJETIVO

Establecer lineamientos y directrices tendientes a asegurar la "confidencialidad, integridad y disponibilidad de los activos de información institucional que apoyan el cumplimiento de su misionalidad, en el marco del cumplimiento de las leyes, decretos, normas políticas del Gobierno Distrital y Nacional relacionadas con la seguridad de la información, seguridad digital y ciberseguridad".

2. ALCANCE

Este manual se enmarca en la Política de Seguridad Digital del Modelo Integrado de Planeación y Gestión – MIPG y comprende todas las actividades que involucran los activos de información, intervenidos por parte de los servidores públicos y colaboradores de la Entidad.

3. ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

La implementación del Modelo de Seguridad y Privacidad de la Información, en desarrollo de las actividades del Sistema de Gestión de Seguridad de la Información en el Instituto para la Economía Social – IPES, requiere garantizar el seguimiento y ejecución de cada una de las tareas que lo consolidan. En ese sentido, a través de la asignación de responsables de seguridad y privacidad de la información, se asigna la ejecución de tareas necesarias para consolidar cada uno de los componentes que dan forma al Modelo de Seguridad y Privacidad de la Información – MSPI.

Por lo anterior, el Instituto para la Economía Social – IPES elaboró un documento, que consolida todos los roles y responsabilidades de los funcionarios, procesos, comités y demás grupos de interés, que hacen parte del Sistema de Gestión de Seguridad de la Información - SGSI, denominado:

- MANUAL DE ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN: ROLES Y RESPONSABILIDADES

4. DEFINICIONES Y SIGLAS[1]

- **Activos de información institucional digital:** Son bienes intangibles de la entidad que se pueden catalogar como la información digital contenida en los sistemas informáticos misionales y administrativos de la entidad, que apoyan el cumplimiento de los objetivos del Instituto para la Economía Social.

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

- **Declaración de aplicabilidad:** Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

- **Evento de seguridad de la información:** Es la presencia identificada de un estado del sistema informático y/o servicio informático y/o de la infraestructura de comunicaciones, que indica un posible incumplimiento de la política de seguridad y/o una falla de controles informáticos, o una situación desconocida que impacte la seguridad de la información institucional digital.

- **Incidente de seguridad de la Información:** Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las actividades del negocio y amenazar la seguridad de la información.

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

- **Política:** Toda intención y directriz expresada formalmente por la dirección.

- **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias

- **Tercera parte:** (Terceros) Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.

[1] Instituto colombiano de Normas Técnicas - ICONTEC Norma Técnica Colombiana NTC-ISO/IEC27002- 2013- 2. Términos y definiciones - 2013, edición digital, pág. 12-14.

- **Directriz:** Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.

- **Servicios de procesamiento de información**: Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan. (sistemas informáticos misional y administrativo, plataforma de correo electrónico institucional, file server, entre otros).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas.

- **Sistema de Gestión de Seguridad de la Información – SGSI:** parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

- **No Repudio:** Se refiere a la capacidad de garantizar que, cuando se realiza un intercambio de información, el receptor de la información no puede negar haberla recibido, y el emisor de la información no puede negar haberla enviado.

- **Malware:** Se replica así mismo al adjuntarse a otro programa o archivo

- **PHISHING, VISHING:** Es una forma de ingeniería social en la cual un atacante intenta de forma fraudulenta adquirir información confidencial, haciéndose pasar por un “tercero de confianza”.

- **Ransomware:** Este malware está diseñado para mantener captivo un sistema de computación o los datos que contiene hasta que se realice un pago

- **Riesgo de seguridad digital:** Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas

involucradas en las actividades y los procesos organizacionales que las soportan.[2]

- **Usuarios:** Funcionarios, contratistas y terceros que tienen acceso a los sistemas de información, servicios de red y a la infraestructura tecnológica que los soporta.
- **CSSI**: Comité de Sistemas y Seguridad de la Información.
- **GOOBI:** Sistemas de Gestión de Recursos Públicos (GIRT)
- **HEMI:** Sistema de Información o Herramienta Misional
- **IT:** Infraestructura Tecnológica
- **MIPG:** Modelo Integrado de Planeación y gestión.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **SDAE:** Subdirección de Diseño y Análisis Estratégico
- **SGSI:** Sistema de Gestión de Seguridad de la Información

5. DESARROLLO

5.1. POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Dirección del INSTITUTO PARA LA ECONOMÍA SOCIAL – IPES, consciente del crecimiento de los riesgos de seguridad digital, derivados del uso y masificación de las tecnologías de información y comunicaciones y considerando que la información es un activo esencial para la toma de decisiones encaminada a mantenerlas al cumplimiento de su misionalidad, se compromete a definir, implementar, y mejorar continuamente el Sistema de Gestión de Seguridad de la Información; de tal forma, que le permita contar con niveles apropiados de integridad, confidencialidad y disponibilidad de sus activos, en el marco del cumplimiento de las leyes, decretos, normas y lineamientos del orden nacional y distrital vigentes; mediante la formulación de objetivos, definición de lineamientos, procedimientos y controles con el propósito de gestionar de manera efectiva

[2] Consejo Nacional de Política Económica y Social –Política de Seguridad Digital CONPES 3854 – 2016 - 3. MARCO CONCEPTUAL, edición digital, pág. 23

los activos de información y sus riesgos.

El Instituto para la Economía Social – IPES gestionará, a través del Comité Institucional de Gestión y Desempeño, los recursos necesarios para mantener el Sistema de Gestión de Seguridad de la Información y reducir los riesgos sobre los activos de información críticos de la entidad; promoverá el compromiso y participación del talento humano y la mejora continua, con el propósito de apropiar una cultura de seguridad de la información en el marco de su misión y objetivos institucionales.

Es obligación de todos los funcionarios y funcionarias, contratistas y terceros con acceso autorizado a la infraestructura tecnológica, servicios de red, aplicaciones y a los activos de información institucional, dar estricto cumplimiento a la política de seguridad y privacidad de la información del Instituto para la Economía Social – IPES.

5.1.1. PRINCIPIOS QUE SOPORTAN EL DESARROLLO DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

a. El IPES establece, comunica y socializa a través de los medios institucionales las responsabilidades asociadas al Sistema de gestión de seguridad de la información, que aplica a todos los funcionarios y funcionarias, contratistas y terceros en el marco del alcance del SGSI.

b. La información derivada del uso de los sistemas y servicios informáticos del Instituto para la Economía Social - IPES (sistema de información misional y administrativo, plataforma de correo electrónico institucional, file server, entre otros) y que sea creada, procesada, modificada y almacenada en la infraestructura será protegida a través de la implementación de controles de seguridad informática que minimicen impactos financieros, operativos o legales.

c. El Instituto para la Economía Social – IPES protege su información de las amenazas asociadas a las tecnologías de información y comunicaciones internas y externas.

d. El Instituto para la Economía Social – IPES controla la operación de sus procesos misionales y administrativos para alcanzar niveles apropiados de seguridad de los recursos tecnológicos y las redes de datos.

e. El Instituto para la Economía Social - IPES implementa controles preventivos que permiten niveles apropiados de disponibilidad de los sistemas y servicios informáticos así como de la continuidad del servicio, mitigando el impacto frente a

la pérdida de activos de información institucional.

f. El Instituto para la Economía Social - IPES desarrolla el Sistema de Gestión de Seguridad de la Información en el marco de la NTC/ISO-IEC 27001, MSPI, MIPG y demás normatividad vigente del orden nacional y distrital.

g. El Instituto para la Economía Social - IPES establece lineamientos y directrices que permiten planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión institucional, los cuales se reflejan en altos estándares de calidad, transparencia, seguridad digital e innovación acorde a las necesidades de los ciudadanos que hacen parte de la población objeto de atención.

h. El Instituto para la Economía Social – IPES aplica los principios de gestión documental, definidos en la entidad y basados en normatividad vigente relacionada, que permiten un uso controlado, clasificación de la información en relación a las directrices de usabilidad, accesibilidad, transparencia, control, conservación, guarda y custodia de los activos de información institucional digital.

5.2. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

a. Gestionar los riesgos de seguridad de la información mediante el análisis de vulnerabilidades, amenazas, criticidad de los activos de información y demás factores que se identifiquen de acuerdo a la metodología y plan de tratamiento utilizados.

b. Aplicar los controles identificados en el plan de tratamiento de riesgos de la empresa, para salvaguardar los activos de información del Instituto para la Economía Social - IPES.

c. Proveer los recursos financieros, recursos de infraestructura y talento humano, necesarios para mantener el Sistema de Gestión de Seguridad de la Información - SGSI.

d. Asegurar el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información mediante la implementación de acciones correctivas, de mejora y planes de acción.

e. Fomentar la conciencia alrededor de la importancia del aseguramiento de la información institucional, la cual debe ser adoptada como una cultura

organizacional.

f. El Instituto para la Economía Social – IPES implementará las medidas que estén a su alcance para salvaguardar la integridad, la disponibilidad, la confidencialidad y la privacidad de la información necesaria para el cumplimiento de su misión.

5.3. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Las medidas de control relacionadas con la seguridad digital, adoptadas por la entidad, en cumplimiento de las disposiciones legales vigentes, del orden distrital y nacional, y las dispuestas por el Comité de Sistemas y Seguridad de la Información, son de obligatorio cumplimiento por parte de los usuarios y usuarias de los sistemas de información y servicios de red de la entidad, quienes son responsables de garantizar la protección de los activos de información institucional.

El desarrollo de la presente política de seguridad y privacidad de la información, así como la definición, implementación, mantenimiento y mejora de los controles de seguridad informática cubren todos los activos de infraestructura tecnológica (servidores, equipos de cómputo, equipos de comunicaciones, entre otros) y a todos los activos de información, (bases de datos, documentos, SIG, servicios informáticos, documentos, registros, entre otros), a fin de proteger la información institucional digital contra daño, pérdida, sustracción, modificación accidental o intencional, describiendo buenas prácticas en el uso de los sistemas y servicios informáticos, así como de los activos de tecnologías de información y comunicaciones, dispuestos por el Instituto para la Economía Social a los usuarios y usuarias para el cumplimiento de sus funciones.

5.4. GESTIÓN DE ACTIVOS

5.4.1. Propiedad Intelectual

La información creada, procesada o modificada haciendo uso de los sistemas y servicios informáticos proporcionados por IPES a los usuarios y usuarias del sistema para el cumplimiento de sus obligaciones, es y permanece como propiedad del Instituto para la Economía Social, y no debe ser copiada, expuesta, sustraída o revelada a terceros.

Para salvaguardar la información institucional como activo de información institucional digital, el Comité de Sistemas y Seguridad de la Información gestionará y dispondrá los

recursos necesarios para su clasificación, valoración, custodia y respaldo, a través de la implementación, mantenimiento y mejora del MIPG.

5.4.2. Confidencialidad

La información creada, procesada, modificada y almacenada en la plataforma tecnológica es propiedad del IPES y es susceptible de clasificación, teniendo en cuenta los lineamientos (modelo de clasificación) para la clasificación de los activos de información institucional. Es responsabilidad de los usuarios y usuarias con acceso autorizado a los activos de información institucional mantener la confidencialidad de los activos de información según su clasificación.

El Instituto para la Economía Social- IPES, incluirá cláusulas de confidencialidad de la información institucional, en los contratos de prestación de servicios, en desarrollo de los procesos de selección. Los usuarios y usuarias que ingresan a la entidad y aceptan las cláusulas de confidencialidad, son responsables del manejo que se dé a los activos de información institucional que cuenten con clasificación reservada o clasificada, lo cual implica restricción en su manejo, uso o divulgación.

5.4.3. Activos de Tecnología de Información y Comunicaciones

Asignación: Todos los activos de infraestructura tecnológica y de comunicaciones del Instituto para la Economía Social dispuesta a los funcionarios y funcionarias, contratistas y terceros, hacen parte del inventario general de la entidad y son asignados oficialmente a los usuarios del sistema, en cumplimiento del documento institucional vigente. Los usuarios y usuarias autorizados son responsables por el manejo que den a los activos que les sean asignados para el cumplimiento de su labor, procurando un uso adecuado a fin de lograr y mantener los niveles apropiados de protección de los mismos.

Devolución de activos: Los usuarios y usuarias de los sistemas y servicios informáticos de la entidad, deben hacer entrega oportuna de los activos de información creados, procesados o modificados durante el vínculo con la entidad debidamente documentados, así como los activos de tecnología asignados por la entidad, en el proceso de terminación laboral.

Infraestructura tecnológica (IT): La Subdirección de Diseño y Análisis Estratégico a través del equipo de Sistemas es responsable de la protección de los activos de infraestructura tecnológica implementada en el centro de datos.

El equipo de sistemas es responsable por la administración de los sistemas y servicios informáticos que soportan la operación tecnológica de la entidad, de acuerdo con el documento institucional y documento de roles y responsabilidades de seguridad y privacidad de la información.

Administración (IT): El equipo de sistemas es responsable de implementar controles que permitan niveles apropiados de disponibilidad de los sistemas y servicios informáticos y de los activos de información institucional. La administración de los medios de procesamiento de información (almacenamiento, virtualización, servidores) es responsabilidad del equipo de sistemas.

- **Backup:** La Subdirección de Diseño y Análisis Estratégico es responsable de realizar copias de respaldo (Backups) de la información institucional contenida en las bases de datos misionales (HEMI), administrativas (GOOBI) y de gestión y de la página web de la entidad.

  El Instituto para la Economía Social- IPES, realizará los esfuerzos de acuerdo al presupuesto para garantizar la integridad de la información almacenada en los sistemas de información críticos, realizando los backup que permitirán realizar la restauración de la información.

  Al interior, la entidad con cada subdirección o área establecerá los parámetros y estrategías con el fin de preservar y conservar la integridad de la información, el uso y respaldo de la misma, dependiendo de la distribución de cada sistema de información.

- **Plan de mantenimiento:** Es responsabilidad del equipo de sistemas realizar mantenimiento y soporte a los equipos de cómputo y periféricos (impresoras, escáner, portátiles, carteleras digitales).

- **Plan de actualizaciones (parches de seguridad):** Es responsabilidad del equipo de sistemas realizar la actualización de parches de seguridad a los servidores con sistema Operativo Microsoft Server cada mes o según los parches que genere Microsoft.

- **Backup de Usuario:** La ejecución de tareas de backup de la información contenida en los equipos de cómputo es responsabilidad de los usuarios y usuarias, de acuerdo a las directrices establecidas por el Instituto para la Economía Social - IPES; el equipo de sistemas realiza tareas de acompañamiento en la forma en cómo

se pueden hacer las copias de seguridad, la regularidad y el medio donde deben ser almacenadas.

5.5. METODOLOGÍA DE VALORACIÓN DE RIESGOS

La valoración del riesgo es el proceso global de análisis y evaluación del riesgo, esta valoración describe cuantitativa o cualitativamente el riesgo y habilita a los encargados del Sistema de gestión de seguridad de la información a priorizar los riesgos de acuerdo a los criterios establecidos. Este proceso realiza las actividades de análisis de riesgo (uso sistemático de la información para identificar las fuentes y estimar el riesgo) y la evaluación de riesgos.

La metodología adoptada por la Entidad y establecida por el Departamento Administrativo de la Función Pública – DAFP en la v5, Guía para la administración del riesgo y el diseño de controles en entidades públicas de fecha diciembre de 2020 y la Política de Administración de Riesgos del IPES.

El IPES define como "**Moderado**" su Nivel de Riesgo Aceptable – NRA para los riesgos de seguridad de la información, por lo tanto, se establecerán planes de respuesta para los riesgos identificados en las zonas "Alto" y "Extremo".

El proceso de gestión de riesgos de seguridad de la información del IPES contiene la siguiente estructura:

- Comprensión del contexto de la gestión del riesgo de seguridad de la información.
- Identificación del riesgo de seguridad de la información.
- Análisis del riesgo de seguridad de la información.
- Evaluación del riesgo de seguridad de la información.
- Tratamiento del riesgo de seguridad de la información.
- Comunicación del riesgo de seguridad de la información.
- Monitoreo y revisión del riesgo de seguridad de la información.

El proceso de gestión de riesgos debe ser registrado en el "Mapa de Riesgos", por parte de cada proceso.

Una descripción detallada de esta metodología se encuentra en:

- INSTRUCTIVO DE GESTIÓN DE RIESGOS SEGURIDAD DE LA INFORMACIÓN

5.6. DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad, es un documento clave e importante para el Sistema de gestión de seguridad de la información. En este documento se detallan los controles implementados en la entidad, alineados con el anexo A, de la norma técnica internacional NTC-ISO-IEC 27001.

La Subdirección de Diseño y Análisis Estratégico, a través del proceso de gestión de seguridad de la información y recursos tecnológicos, por medio de la administración de la plataforma tecnológica, realiza la implementación, mantenimiento y mejora de los controles de seguridad informática a partir del análisis de riesgos y requisitos legales.

La descripción de los controles implementados en la declaración de aplicabilidad de la entidad, se encuentra en el documento "SOA-IPES", y se encuentra disponible en la Subdirección de Diseño y Análisis Estratégico, proceso de gestión de Seguridad de la información y recursos tecnológicos.

5.7. POLÍTICAS OPERATIVAS DEL SGSI

5.7.1. Política de uso de correo electrónico y usuarios de red Objetivo:

Definir los lineamientos generales para asegurar la protección de los activos de información, asociada al uso del correo electrónico institucional y al usuario de red, por parte de los usuarios y usuarias autorizadas.

Aplicabilidad:

La política de uso del correo electrónico institucional y usuario de red aplica a toda la entidad y a todos los usuarios y usuarias autorizados para acceder al servicio.

Los usuarios y usuarias autorizados para usar el servicio de correo electrónico y usuario de red son responsables de mantener un comportamiento ético y acorde a la ley, así como de evitar prácticas o usos que puedan comprometer la seguridad de la información de la entidad.

El servicio debe ser empleado para servir a una finalidad operativa y administrativa en relación con el Instituto para la Economía Social. Todas las comunicaciones establecidas

mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad del Instituto y podrán ser monitoreadas por el administrador del servicio y revisadas por las instancias de vigilancia y control distritales y nacionales. El incumplimiento de la presente política puede conducir a acciones disciplinarias tales como terminación de la relación laboral o acciones de índole legal.

Detalle de la Política:

La creación de una cuenta de correo electrónico institucional y usuario de red deben ser autorizadas por el/la Director/a, Jefes de Oficina, y/o Subdirectores/as a la cual pertenezca cada usuario y usuaria, a través del formato institucional vigente. Dicho formato valida la asignación de perfiles y/o roles que el usuario o usuaria desarrollará en la entidad. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desempeñada y no debe usarse para ningún otro fin.

Las contraseñas de los correos electrónicos institucionales se encontrarán sincronizadas con el usuario de red. Es responsabilidad de los usuarios y usuarias mantener su contraseña de forma segura y no revelarla, ya que la misma es personal e intransferible.

Los funcionarios y funcionarias, contratistas y demás colaboradores que sean autorizados para usar este servicio, no deben considerar que los mensajes que envían o reciben en su cuenta de correo electrónico sean confidenciales a no ser que sea establecido expresamente por la entidad.

Todo usuario usuaria es responsable por la destrucción de todo mensaje cuyo origen es desconocido, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos.

Los correos electrónicos deben contener una sentencia de confidencialidad ubicada al final del texto, después de la firma del mismo.

Todo usuario o usuaria es responsable de informar los contenidos o accesos a servicios que no le estén autorizados o no correspondan a sus funciones dentro del IPES.

Es responsabilidad del **Área de Talento Humano** informar oportunamente al administrador del servicio, sobre el retiro de la entidad de **funcionarios y funcionarias** a quienes se haya asignado una cuenta de correo institucional y usuario de red.

Es responsabilidad de los **perfiles directivos** de las dependencias del IPES informar

oportunamente al administrador del servicio, sobre el retiro de la entidad de los **contratistas** a quienes se haya asignado una cuenta de correo institucional y usuario de red.

Los usuarios del servicio que se retiren de la entidad deben abstenerse de continuar aplicándolas y deberá verificar que su cuenta y acceso a los servicios sean cancelados.

El servicio de correo electrónico no debe ser utilizado para:

- Envío de correos masivos.
- Envío, reenvío o intercambio de mensajes no deseados o considerados SPAM, cartas en cadena o publicidad.
- Envío de correos con archivos adjuntos de gran tamaño que puedan causar congestión en la red o que no puedan ser recibidos por la cuenta destinataria.
- Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, o con contenidos sexistas, racistas, políticos, pornográficos, difamatorios, terroristas, entre otros.
- Creación, almacenamiento o intercambio de mensajes que violen las leyes de material protegido por la ley de derechos de autor.
- Distribuir información institucional, valorada como reservada o clasificada, a otras entidades o ciudadanos sin la debida autorización.
- Crear, enviar, alterar, borrar mensajes de un usuario o usuaria sin su autorización.
- Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario o usuaria como si fuera propia sin la debida autorización.
- Cualquier otro propósito inmoral o ilegal.

El servicio de usuario de red debe tener en cuenta para las siguientes condiciones:

- Usar claves seguras robustas y complejas, crearlas de 8 caracteres y que incluyan: mayúsculas, minúsculas, números y símbolos, que no sea número de documento de identidad, nombres y apellidos.
- El usuario de red aplica para el acceso de las plataformas de los servicios de la entidad

tales como Mesa de Ayuda, HeMi, Suite Visión Empresarial (SVE) y los equipos de cómputo de la entidad pública y así mismo el acceso de las carpetas de los servidores y el escritorio remoto (VPN).

- No divulgar ni compartir la clave a los demás ya que cuenta el permiso y roles para ciertas funciones competentes y por la seguridad de la información.

Responsabilidades

El Proceso de Gestión de la Información y Recursos Tecnológicos - PGIRT es responsable de administrar la plataforma tecnológica que soporta el acceso al servicio de correo electrónico corporativo y usuario de red para los funcionarios, contratistas y demás colaboradores que desempeñen labores en el Instituto para la Economía Social.

5.7.2. Política de Uso de Internet Objetivo:

Definir los lineamientos generales para asegurar la protección de los activos de información institucional, asociada al uso de Internet, por parte de los usuarios autorizados.

Aplicabilidad:

La política de uso de internet aplica a toda la entidad y a todos los usuarios y usuarias autorizados para acceder al servicio.

Los usuarios y usuarias autorizados para usar el servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer la seguridad de los activos de información del IPES.

El servicio debe ser empleado para servir a una finalidad operativa y administrativa en relación con el Instituto para la Economía Social. Todas las comunicaciones establecidas mediante este servicio pueden ser escaneadas por el administrador del servicio o revisadas por cualquier instancia de vigilancia y control distrital o nacional.

Detalle de la Política.

Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la entidad y no debe utilizarse para ningún otro fin.

Todo usuario o usuaria es responsable tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la red de datos.

Los usuarios y usuarias autorizados no podrán descargar software que se encuentre protegido con derechos de autor.

El acceso a redes sociales estará restringido; los usuarios y usuarias que requieran acceder a estas categorías, deberán informar al administrador de la plataforma sobre la necesidad, previa autorización del jefe directo.

Este servicio no debe ser usado para:

- Envío o descarga de información de gran tamaño que pueda congestionar la red.
- Envío, descarga o visualización de información con contenidos que atenten contra la integridad moral de las personas o instituciones.
- Acceso a páginas web, portales, sitios web o aplicaciones web que no hayan sido autorizadas.
- Cualquier otro propósito considerado inmoral o ilegal.

Responsabilidades

Todos los funcionarios y funcionarias, contratistas y terceros que interactúan en el desarrollo de sus tareas habituales u ocasionales, que utilicen cualquier servicio de tecnología de la información y comunicaciones (TIC) que provea el Instituto para la Economía Social son responsables del cumplimiento y seguimiento de esta política.

El equipo de Sistemas - SDAE es el responsable de administrar la plataforma tecnológica que soporta el acceso a Internet para los funcionarios y funcionarias, contratistas y demás colaboradores que desempeñen labores en la entidad.

El equipo de Sistemas - SDAE se reserva el derecho de escanear las comunicaciones o información que presenten un comportamiento inusual o sospechoso.

El equipo de Sistemas - SDAE se reserva el derecho de filtrar los contenidos que se reciban desde Internet, o se envíen desde la red del IPES.

5.7.3. Política de Seguridad de Control de Acceso.

Objetivo:

Controlar y/o limitar el acceso físico y lógico a la información, a los servicios de procesamiento de información, a los sistemas y servicios informáticos y de red del Instituto para la Economía Social
- IPES, así como evitar la exposición de activos de información y medios de procesamiento de información a daño, pérdida, robo o modificación accidental o intencional.

Aplicabilidad:

Esta política aplica a todos los funcionarios y funcionarias, contratistas y terceros interesados del Instituto para la Economía Social IPES, que usen su infraestructura y accedan a sus activos de información.

Detalle de la política:

El Instituto para la Economía Social proporciona a los funcionarios y funcionarias, contratistas y terceros con acceso autorizado, los recursos tecnológicos necesarios para que puedan desempeñar sus funciones, por tal motivo no se permite conectar a la red dispositivos (portátiles, celulares, tablets, enrutadores, agendas electrónicas, puntos de acceso inalámbrico) que no sean autorizados por el Comité de Sistemas y Seguridad de la información.

Sin excepción, los accesos a los activos de información del Instituto para la Economía Social – IPES, deberán cumplir con los requisitos legales, normativos, reglamentarios, procedimentales o que hayan sido determinados por el responsable del activo de información para un uso seguro del mismo.

Para propósitos de control e investigación de eventos o incidentes de seguridad de la información se podrán auditar los registros de acceso y actividades desarrolladas en los sistemas de información y áreas seguras del Instituto para la Economía Social IPES. Los accesos y/o utilización de los activos de información del Instituto para la Economía Social - IPES se deben registrar para garantizar la trazabilidad de las acciones realizadas, identificando, entre otros datos relevantes, quién realiza el acceso y las operaciones realizadas.

Los funcionarios y funcionarias, contratistas o terceros, no deben realizar modificaciones a la información o los activos de información sin la debida autorización del dueño o custodio del activo de información.

Los funcionarios y funcionarias, contratistas y terceros, tienen la responsabilidad de mantener la integridad, confidencialidad y disponibilidad de la información, los activos de información y los sistemas informáticos a los cuales se les han concedido accesos o han designados y autorizados, asegurándose que éstos sólo sean utilizados para el desarrollo de las labores encomendadas.

Todos los activos de información o sistemas de información del Instituto para la Economía Social - IPES deben tener asignado un responsable, custodio o líder de área; quien otorgará la autorización para el acceso a la información contenida en el mismo.

El acceso a la información y los activos de información del Instituto para la Economía Social - IPES es controlado conforme a los roles y responsabilidades de los funcionarios y funcionarias, contratistas o terceros interesados, para poder ejecutar la función designada.

Para un efectivo uso y custodia de los activos de información del Instituto para la Economía Social
- IPES, al autorizar los accesos se debe considerar el nivel de clasificación legal asignado al activo de información según el procedimiento de clasificación y etiquetado de la información de la Entidad. Por lo que la información de naturaleza pública debe estar disponible a la ciudadanía; para la demás información debe mediar solicitud expresa y se entregará al peticionario o peticionaria, siempre y cuando no esté sometida a reserva legal o existan restricciones para su acceso.

Todo acceso físico o lógico otorgado a los funcionarios y funcionarias, contratistas o terceros debe ser desactivado, revocado o modificado una vez se termine la autorización de uso sobre estos o exista desvinculación laboral del Instituto para la Economía Social - IPES.

Por parte de los perfiles directivos deberán verificar periódicamente las novedades del personal (funcionarios y funcionarias, contratistas y terceros), validar la eliminación, reasignación o bloqueo de las cuentas de acceso de los recursos tecnológicos y sistemas de información.

Los funcionarios y funcionarias y los contratistas deberán realizar la devolución del carné

institucional a la Oficina Asesora de Comunicaciones - OAC tan pronto el personal termine su vinculación con la entidad, condición para la firma del paz y salvo.

5.7.4. Política de Seguridad de Control de Acceso Lógico:

Objetivo:

Controlar y/o limitar el acceso lógico a la información, a los servicios de procesamiento de información, a los sistemas y servicios informáticos y de red del Instituto para la Economía Social - IPES.

Aplicabilidad:

Esta política aplica a todos los funcionarios y funcionarias, contratistas y terceros interesados del Instituto para la Economía Social - IPES, que usen servicios o sistemas de información.

Detalle de la política:

La Subdirección de Diseño y Análisis Estratégico es responsable de suministrar a los usuarios y usuarias las contraseñas de acceso a los servicios de red y sistemas de información en concordancia con el rol definido, las cuales son de uso personal e intransferible y no debe ser revelada, expuesta o compartida.

Se deberá asignar un nombre de usuario para conceder el acceso a los sistemas de información.

Es responsabilidad de los perfiles directivos solicitar la autorización de la asignación de credenciales de usuario, a través del cual se compromete a mantener la confidencialidad de las mismas.

Solo personal designado por Gestión de la Información y Recursos Tecnológicos (GIRT) está autorizado para realizar instalaciones de software sobre la infraestructura tecnológica dispuesta a los usuarios y usuarias del sistema, para lo cual se dispondrá de las credenciales de administrador o administradora.

Es responsabilidad del equipo de sistemas mantener niveles de seguridad apropiados asociados a la cuenta administrador o administradora.

Los usuarios y usuarias con acceso autorizado a la plataforma tecnológica y áreas de la

entidad, son responsables por el manejo y el tratamiento que se dé a los activos de información institucional, dependiendo de los roles y responsabilidades establecidas. Es responsabilidad de los usuarios y usuarias dar estricto cumplimiento a la política de tratamiento de datos establecida en el Instituto para la Economía Social – IPES.

El sistema de información misional debe contar con perfiles de usuario, los cuales permitan el acceso a la información y funcionalidades, en concordancia con los roles y responsabilidades de los usuarios y usuarias.

Las áreas misionales son responsables por el análisis, manejo y tratamiento que se dé a la información institucional derivada del uso del sistema de información misional (HeMi) al igual que las demás dependencias de la entidad sobre el sistema de información administrativo y financiero (Goobi GRP). Gestión de la Información y Recursos Tecnológicos (GIRT), en cabeza de la Subdirección de Diseño y Análisis Estratégico es responsable de la guarda y custodia de la información alojada en el sistema de información misional y el sistema de información administrativo y financiero.

La conexión remota a los servicios informáticos de la entidad, se realiza únicamente a través de una conexión VPN (Red Privada Virtual) segura suministrada por la entidad, previa solicitud formal del jefe o de la jefe directa y revisión y autorización del Comité de Sistemas y Seguridad de la Información.

Gestión de la Información y Recursos Tecnológicos (GIRT) podrá realizar monitoreo a las conexiones externas.

Es responsabilidad del Área de Talento Humano informar oportunamente a Gestión de la Información y Recursos Tecnológicos (GIRT), las novedades relacionadas con los usuarios y usuarias de la plataforma tecnológica de la entidad, a fin de ejercer un efectivo control sobre los privilegios de acceso.

Es responsabilidad de la Gestión de la Información y Recursos Tecnológicos (GIRT), en desarrollo de la administración de los activos de información (*equipos de cómputo, sistema de información, bases de datos, repositorios de archivos, licencias, etc*.), a intervalos regulares, realizar monitoreo periódico y depuración de los privilegios de acceso asignados a los usuarios y usuarias autorizados.

5.7.5. Política de Seguridad de Control de Acceso Físico:

Objetivo:

Controlar y/o limitar el acceso físico a la información, a los servicios de procesamiento de información, a los sistemas y servicios informáticos y de red del Instituto para la Economía Social IPES, así como cualquier activo de información identificado por la entidad.

Aplicabilidad:

Esta política aplica a todos los funcionarios y funcionarias, contratistas y terceros interesados del Instituto para la Economía Social IPES, que usen servicios o sistemas de información e infraestructura tecnológica.

Detalle de la política:

Toda persona (funcionario y funcionaria, contratista, tercero interesado o visitante) se deberá identificar en la entrada principal del edificio con el personal de vigilancia y el área de recepción para realizar el respectivo registro; en caso de requerir acceso a las áreas seguras se debe identificar con el o la líder o responsable del área segura del Instituto para la Economía Social - IPES a fin de autorizar su ingreso y conceder los privilegios necesarios para el acceso físico.

Se deberá contar con mecanismos de control de acceso físico para las áreas seguras identificadas por el Instituto para la Economía Social - IPES (el centro de cómputo y oficinas que almacenen información reservada); tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras y dar estricto cumplimiento al procedimiento de trabajo en áreas seguras.

Las puertas de acceso a las áreas identificadas como seguras o que alberguen activos de información críticos, sensibles o confidenciales, deberán permanecer siempre cerradas y aseguradas con llave. De igual manera, los gabinetes y archivadores que contienen archivos físicos en cada área deberán permanecer cerrados, en especial cuando no haya funcionarios o funcionarias en las oficinas donde reposa la información física.

Se deberá aprobar de manera previa las solicitudes de acceso de terceros al centro de cómputo o a los centros de cableado, además se deberá acompañar permanentemente a los y las visitantes durante su estancia en las áreas mencionadas.

Se deberá registrar el ingreso de los y las visitantes al centro de cómputo y a los centros

de cableado en una bitácora ubicada en la entrada de estos lugares de forma visible.

Se deberá monitorear permanentemente los ingresos a las áreas seguras, para identificar posibles accesos no autorizados y para confirmar que los controles de acceso son efectivos.

De conformidad con el artículo 34 de la ley 734 de 2002 son deberes de todo servidor y servidora pública: "Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida".

De conformidad con el artículo 35 de la ley 734 de 2002 a todo servidor o servidora pública le está prohibido: "Dar lugar al acceso o exhibir expedientes, documentos o archivos a personas no autorizadas".

En cumplimiento del Artículo 4°. Principios para el Tratamiento de datos personales de la ley 1581 de 2012 y en lo específico al principio de confidencialidad: todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

5.7.6. Política de Seguridad de Escritorio y Pantalla Limpia.

Objetivo:

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario y trabajo normal de los usuarios y usuarias, en escritorios y áreas de trabajo.

Aplicabilidad:

Esta política aplica a todos los funcionarios y funcionarias y contratistas de la entidad, que hagan uso de la infraestructura tecnológica y áreas del Instituto para la Economía Social.

Detalle de la política:

Con el fin de establecer controles para el aseguramiento de la información del Instituto de Economía Social – IPES, los funcionarios y funcionarias y/o contratistas deben adoptar

buenas prácticas para el manejo y administración de la información física y electrónica que se encuentra a su cargo, a fin de evitar que personas no autorizadas accedan a la misma. Para ello, los funcionarios y funcionarias, contratistas o terceros deben cumplir los siguientes lineamientos:

El personal del Instituto para la Economía Social - IPES debe conservar su escritorio libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento y mantener en su puesto de trabajo únicamente la información con la que está trabajando en el momento, de igual forma no deje notas en el monitor o en cualquier otro espacio visible con información clasificada y/o reservada.

Los funcionarios y funcionarias y/o contratistas deben guardar en forma segura documentos y elementos de almacenamiento externos como (CD, DVD, USB, equipos portátiles, entre otros) en especial cuando no se encuentren en sus sitios de trabajo; para evitar accesos no autorizados, pérdida o daño de la información.

Evitar guardar en el escritorio o pantalla inicial del computador los archivos que contengan información sensible o confidencial, por lo que deberán ser almacenados en rutas que impidan el fácil acceso a terceros a fin de evitar fugas de información del Instituto para la Economía Social - IPES.

Es responsabilidad de los usuarios y usuarias bloquear la sesión de usuario en el computador donde realice su autenticación, con el protector de pantalla designado por la entidad, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su sitio de trabajo.

Los equipos de cómputo deberán quedar apagados al finalizar la jornada laboral o cuando una ausencia temporal supere las cuatro horas.

Al imprimir documentos de carácter público reservado o público clasificado, deben ser retirados de la impresora inmediatamente.

No imprimir trabajos o documentos que no sean del Instituto para la Economía Social IPES

Los equipos tecnológicos que generalmente pueden estar desatendidos como escáneres, fax o fotocopiadoras, deberán ser autorizados para su uso.

El Comité de Sistemas y Seguridad de la Información o el Oficial de Seguridad de la Información determinarán los controles de bloqueo sobre las sesiones de los usuarios y

usuarias para que el equipo se bloquee en un lapso de tiempo determinado.

No está autorizado modificar el fondo del escritorio o protector de pantalla, ya que estos son de uso institucional.

Los funcionarios y funcionarias, contratistas o terceros que tengan dentro de sus responsabilidades la atención al público, deben almacenar los documentos y dispositivos de almacenamiento móviles bajo llave; y ubicar el equipo de cómputo de tal forma que se evite el acceso o revisión de la información por parte de las personas no autorizadas.

5.7.7. Política de Seguridad de Copias de Respaldo y Restauración.

Objetivo:

Definir las directrices para la administración y custodia de los medios de respaldo del Instituto para la Economía Social – IPES, con el fin de asegurar que la disponibilidad e integridad de todo software e información esencial se pueda recuperar después de una falla o incidente de fuerza mayor.

Aplicabilidad:

Esta política será aplicada por los administradores de tecnología, encargados de sistemas de información, usuarios finales y jefaturas de área que decidan sobre la disponibilidad e integridad de los datos.

Detalle de la política:

La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento definido por la entidad, como por ejemplo: discos magnéticos, discos flash, drive, entre otros, de acuerdo a los requisitos legales, las directrices internas del Instituto para la Economía Social - IPES, el análisis y tratamiento de los riesgos, clasificación de información y nivel de criticidad de la misma.

Los administradores de los servicios tecnológicos, los sistemas de información o los equipos de comunicación en compañía del dueño o dueña de la información, serán los responsables de definir la frecuencia de respaldo y definir los requerimientos de seguridad de la información; el administrador o administradora del sistema de respaldo en conjunto con el equipo de sistemas del IPES serán responsables de realizar las pruebas de respaldo periódicas, para garantizar la disponibilidad de las mismas de acuerdo con el plan de contingencia para los sistemas de información que hace parte del **Plan de Contingencia TI y el Plan de Recuperación Ante Desastres**.

También este proceso le implica al IPES y en especial al administrador o administradora del sistema de backup que todas las copias de información crítica deben ser almacenadas en un área adecuada y que cuente con control de acceso tanto físico como lógico, para evitar que sean manipuladas por personal no autorizado, igualmente que se custodie estos backups en una zona diferente al del data center principal.

Los tiempos de preservación de las copias de respaldo deben ser definidos teniendo en cuenta los requerimientos de los procesos institucionales, la tecnología requerida para la restauración de la información, el tipo de información que contienen las copias de respaldo y la criticidad que representan para cada uno de los procesos, se debe tener en cuenta el documento de preservación de digital a largo plazo.

Cuando se requiera la realización de copias de respaldo en algunas de las áreas o subdirecciones, diferentes a las ya definidas por el Comité de Sistemas y Seguridad o los Administradores TI, el o la responsable de la información debe formular un requerimiento a la Subdirección de Diseño y Análisis Estratégico, determinando la necesidad del respaldo de información, el tipo de información a copiar, frecuencia requerida para la utilización de la copia de respaldo, niveles de calificación de la información y el tiempo de retención de las copias.

Al cumplir el ciclo de vida útil de los medios de almacenamiento de las copias de respaldo, estos medios deben ser eliminados o sometidos a disposición final de forma segura, evitando la recuperación de la información contenida y acceso por personas no autorizadas. Los procesos de eliminación o disposición final deben cumplir con la normatividad vigente en materia de dispositivos de residuos electrónicos.

Los funcionarios y funcionarias, contratistas o partes interesadas responsables de la infraestructura, sistemas de información y bases de datos requeridas para la operación de los procesos institucionales, deben generar las respectivas copias de respaldo, estableciendo la periodicidad, tipo de almacenamiento, herramienta utilizada y registrando la información según lo establecido dentro de la presente política; y verificar que dichas copias se ajusten a las necesidades y requerimiento del Instituto para la Economía Social – IPES.

Los responsables de la información en cada estación de trabajo, serán los encargados de realizar las copias de respaldo de su información y verificar que se realicen de acuerdo con lo establecido en el presente manual *(9.3 Activos de Tecnología de Información y Comunicaciones – Backup de Usuario, y el Procedimiento BACKUP GENERACIÓN Y*

RECUPERACIÓN) y que dichas copias se ajusten a las necesidades y requerimientos misionales del Instituto para la Economía Social - IPES.

El Comité de Sistemas y Seguridad de la Información o los Administradores TI definirán la ubicación y forma de guardar la información en los equipos de cómputo de los funcionarios y funcionarias y contratistas, de tal forma, que facilite la identificación de la misma en el momento de realizar las copias de respaldo; de igual forma, los funcionarios y funcionarias y contratistas son responsables de depurar la información para la optimización de los recursos institucionales.

Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de una infección de virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, por requerimientos legales o cualquier catástrofe que esté listada en el **Plan de Contingencia TI y el Plan de Recuperación Ante Desastres**.

Un plan de emergencia debe ser desarrollado para todas las aplicaciones misionales que manejen información crítica, el dueño o dueña de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.

5.7.8. Políticas Específicas de usuario o usuaria.

Objetivo.

Definir lineamientos generales para asegurar una adecuada protección de los activos de información del Instituto para la Economía Social – IPES por parte de los usuarios y usuarias de la entidad.

Aplicabilidad.

Estas políticas aplican a todos los funcionarios y funcionarias, contratistas y terceros que cuenten con algún vínculo vigente con la entidad.

Detalle de la Política.

El Instituto para la Economía Social – IPES dispone de un espacio de almacenamiento de la información en un servidor de archivos con los permisos necesarios para que cada usuario o usuaria guarde la información importante y sobre ella se garantizará la

disponibilidad en caso de un daño en el equipo asignado al usuario o usuaria, esta información será guardada de acuerdo a las tablas de retención documental de la entidad.

El personal del proceso de gestión de seguridad de la información y recursos tecnológicos (Sistemas), es el único autorizado para realizar instalación de los programas que han sido adquiridos por la entidad, en los equipos de los usuarios o usuarias, teniendo en cuenta roles y responsabilidades. El uso de programas obtenidos a partir de otras fuentes (software o música), puede implicar amenazas legales y de seguridad a la entidad, por lo que dicho uso está estrictamente prohibido. El Instituto para la Economía Social - IPES no se hace responsable por las copias no autorizadas.

El uso de dispositivos de almacenamiento como DVD, CD, memorias USB, agendas electrónicas, celulares, tabletas y teléfonos inteligentes entre otros, pueden ocasionalmente generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para fuga de información, por lo que su uso no es permitido. Los usuarios y usuarias que requieran hacer uso de dispositivos tecnológicos que no hacen parte del inventario de la entidad, deberán ser autorizados por el subdirector, subdirectora o jefe de oficina.

Los programas instalados en los equipos de cómputo de la entidad, son de propiedad del Instituto para la Economía Social - IPES, la copia no autorizada de programas legales o de su documentación, implica una violación a la presente política. Aquellos empleados que utilicen copias no autorizadas de programas y su respectiva documentación, quedarán sujetos a las acciones disciplinarias o legales establecidas por el Instituto para la Economía Social - IPES y demás entes rectores de seguridad de la información.

El Instituto para la Economía Social – IPES se reserva el derecho de proteger su reputación y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso y las copias no autorizadas de los programas. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.

Los recursos tecnológicos y de software asignados a los funcionarios y funcionarias del Instituto para la Economía Social - IPES son responsabilidad de estos.

Ninguna clase de información de tipo electrónico de la entidad debe almacenarse en los discos duros de los computadores personales de los empleados o empleadas. Se deben utilizar las unidades creadas y asignadas por la Subdirección de Diseño y Análisis Estratégico para estos propósitos.

Los usuarios y usuarias son responsables y asumen las consecuencias por la pérdida de información que esté bajo su custodia. Se prohíbe el almacenamiento de información personal en los computadores del Instituto para la Economía Social - IPES y en el correo institucional, el escritorio lógico (del computador) debe estar libre de información pública clasificada e información pública reservada.

Los usuarios y usuarias sólo tendrán acceso a la información, datos y recursos autorizados por el Instituto para la Economía Social - IPES, y serán responsables por la divulgación no autorizada de esta información.

La información realizada o gestionada durante el término de su contrato, debe ser almacenada en el drive del correo institucional y en el drive compartido por cada área.

Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., que son el resultado de los procesos informáticos, así como los datos de entrada a los mismos.

Los recursos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.

Los equipos que se encuentren fuera de las instalaciones del IPES, no deben dejarse en sitios públicos sin una adecuada vigilancia.

Cualquier incidente o posible evento que afecte la seguridad de la información debe ser reportado inmediatamente al equipo de sistemas, o a la mesa de ayuda o al área designada para este fin.

El personal de la entidad debe ser consciente que debe tomar las precauciones necesarias para no revelar información no pública cuando se hace una llamada telefónica que puede ser interceptada mediante acceso físico a la línea o al auricular o escuchada por personas que se encuentren cerca.

Lo anterior debe aplicar también cuando el empleado o empleada se encuentre en sitios públicos como restaurantes, transporte público o ascensores.

La conexión remota a la red de datos de la entidad, se debe establecer a través de una conexión VPN (Red Privada Virtual) segura, suministrada por la entidad, la cual debe ser aprobada por el Comité de Seguridad de la Información, registrada y auditada.

5.7.9. Políticas específicas del personal de tecnología.

Objetivo:

Definir lineamientos y directrices para asegurar una adecuada protección de los activos de información institucional, por parte de los administradores y administradoras de la plataforma tecnológica que soporta la operación informática de la entidad.

Aplicabilidad:

Estas políticas aplican al personal del proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, y al personal que esté encargado de un sistema de información de la entidad.

Detalle de la Política:

Toda licencia y sus medios se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.

Disponer de los procedimientos relacionados con la administración y operación tanto de la de la plataforma tecnológica como de los servicios de información.

Deberá vigilar y llevar un inventario detallado de la infraestructura de Hardware del Instituto para la Economía Social - IPES, acorde con las necesidades existentes de la misma. Las copias licenciadas y registradas del software adquirido deben ser únicamente instaladas en los equipos de cómputo y activos de infraestructura tecnológica (servidores, firewall, almacenamiento) de la entidad.

Mantener custodiadas las claves de acceso a cada uno de los servicios de tecnología.

No está permitido hacer copias de programas o su documentación sin el consentimiento por escrito del Instituto para la Economía Social - IPES y del proveedor del software.

Por defecto, en los servidores, todos los protocolos y servicios deben ser bloqueados, no se debe permitir ninguno a menos que sea solicitado por el área responsable y aprobado por el área de Sistemas.

Servicios y procedimientos informáticos no esenciales y que no se puedan asegurar no serán permitidos.

El acceso a cualquier servicio o a algún servidor o sistema de información debe ser autenticado, autorizado y auditado.

Todos los servidores deben ser configurados con el mínimo de servicios asegurados para desarrollar las funciones designadas.

Pruebas de laboratorio, pruebas de sistemas de información, pruebas de software tipo freeware o shareware o pruebas de sistemas que necesiten conexión a internet, deben ser realizadas sin conexión a la red LAN de la entidad y con una conexión separada de internet o en su defecto con una dirección IP diferente a las direcciones públicas de producción.

Dentro del sistema autónomo de interconexión de redes de la entidad, deben establecerse los controles necesarios de enrutamiento así como la autenticación del protocolo de enrutamiento cuando el dispositivo lo permita.

Aplicar la metodología para establecer los patrones de uso de correo electrónico e internet (Anexo 3) de la resolución 305 de 2008 de la Comisión Distrital de Sistemas.

5.7.10. Política de Gestión de Incidentes de Seguridad de la Información.

Objetivo:

Proteger la integridad, disponibilidad y confidencialidad de los activos de información de la entidad, prevenir la pérdida de servicios y cumplir con requerimientos legales. Esta política establece los mecanismos de coordinación para dar respuesta a los incidentes de seguridad y habilita a la entidad para una remediación rápida, recopilación de datos y reporte de los eventos que afectan la infraestructura de información y tecnología.

Aplicabilidad:

Un incidente de seguridad de la información es cualquier evento desconocido que daña o representa una amenaza seria para toda o una parte de la infraestructura tecnológica, servicios de red, de procesamiento de información y a los activos de información de la entidad (sistemas de cómputo, de información y de telefonía), como pueden ser: ausencia de servicios, inhibición para el uso de sistemas de información, incluyendo cambios no autorizados al hardware, firmware, software o datos, crímenes definidos en la ley 1273 de 2009 u otras normas que acojan a la entidad.

Un sistema de información es cualquier equipo de cómputo o telecomunicaciones, sistema y/o Sistema interconectado o no conectado usado para la adquisición, almacenamiento, manipulación, gestión, movimiento, control, despliegue, conmutación, intercambio, transmisión o recepción de voz, datos, vídeo en formas análogas o digitales, así como el software, firmware o hardware que forme parte del sistema.

La política permite establecer las directrices para gestionar, dar respuesta, documentar y reportar los incidentes de seguridad de la información que afectan a la infraestructura de información y comunicaciones de la entidad. Los incidentes incluyen eventos como: sustracción de información, intrusión a sistemas de información, uso no autorizado de datos, denegación de servicios, violación a las políticas de uso de servicios como correo y otras actividades contrarias a las políticas de uso adecuado de recursos de información y tecnología de la entidad.

La política se aplica a funcionarios y funcionarias, contratistas, proveedores y todo personal que tenga acceso a los activos de información e infraestructura tecnológica institucional, así como a todos los recursos de información y tecnología empleados para la prestación de servicios de la entidad.

La política de gestión de incidentes de seguridad de la información de la entidad y sus procedimientos de apoyo definen los métodos estándar para identificar, realizar seguimiento y responder a los incidentes de seguridad de la información de la entidad.

Detalle de la Política:

Es responsabilidad de los funcionarios y funcionarias, contratistas o entidades externas reportar eventos relacionados con la seguridad de la información al oficial de seguridad de la información del Instituto para la Economía Social - IPES. El o la oficial de seguridad de la información por sí mismo también puede identificar incidentes a través de supervisión proactiva de los sistemas de información y tecnología de la entidad. Una vez identificado el incidente el oficial de seguridad de la información utilizará el procedimiento interno aprobado para registrar y realizar seguimiento a los incidentes y trabajar con otros funcionarios y funcionarias u organizaciones para tomar las acciones apropiadas como investigar, escalar, remediar, referenciar el incidente a otras organizaciones como lo establece el procedimiento de respuesta a incidentes de seguridad de la información.

Cualquier dispositivo de uso personal como teléfonos inteligentes, computadores portátiles, handhelds, u otros dispositivos de cómputo que estén implicados en incidentes de seguridad pueden ser sometidos a cadena de custodia o retención para fines de

investigación o evidencia ante procesos legales. En caso de usar ese tipo de dispositivos, sus propietarios o propietarias aceptan formalmente las políticas de seguridad institucionales.

Responsabilidades:

El o la oficial de seguridad de la información es responsable por el aislamiento y recuperación de los accesos a sistemas de comunicaciones y cómputo afectados por el incidente. El o la oficial de seguridad de la información debe conformar un equipo para la atención y respuesta a incidentes; de acuerdo con la naturaleza del incidente pueden ser convocados: Niveles directivos de la entidad, áreas de control interno de la entidad, equipos jurídicos o técnicos especializados.

El o la oficial de seguridad de la información debe garantizar que los incidentes sean apropiadamente registrados y almacenados de acuerdo con los procedimientos de control de registros del proceso de gestión de seguridad de la información. Los reportes de incidentes deben ser remitidos por el oficial de seguridad de la información al Comité de Sistemas y Seguridad de la entidad o el designado por la entidad, el oficial de seguridad de la información o el equipo de respuesta a incidentes, son responsables de comunicar al personal pertinente las etapas y acciones que se siguen para dar respuesta al incidente.

El plan de respuesta o remediación específico para un incidente pueden ser suministrado por requerimiento específico o por iniciativa del Instituto para la Economía Social - IPES a organismos de seguridad, control o respuesta a incidentes de seguridad del estado con el fin de evaluar su efectividad, solicitar apoyo, demostrar debida diligencia u otros propósitos definidos por la entidad.

Cuando sea viable, el IPES adoptará procedimientos para llevar a cabo actividades de prevención de incidentes, supervisión y filtrado de anomalías que puedan afectar a la seguridad de la información o los recursos de información y tecnología de la entidad.

El o la oficial de seguridad de la información de la entidad debe mantener procedimientos para registro, seguimiento y reporte de incidentes. El o la oficial de seguridad de la información mantendrá los procedimientos para la respuesta e investigación de los diferentes tipos de incidentes de seguridad de la información, así como asegurar la custodia de las evidencias obtenidas durante la investigación.

5.7.11. Políticas Generales del Negocio.

Objetivo:

Definir los lineamientos y directrices de propósito general del negocio para asegurar una adecuada protección de la información del Instituto para la Economía Social - IPES.

Aplicabilidad:

Estas son políticas que aplican a la dirección, subdirecciones, jefes de oficinas asesoras, responsables del Sistema Integrado de Gestión y área de Sistemas para cumplir con los propósitos generales del negocio del Instituto para la Economía Social.

Detalle de la política:

Diseñar, programar y realizar por parte de la Asesoría de Control Interno (ACI), los programas de auditoría del Sistema de Gestión de Seguridad de la Información.

La Dirección del Instituto para la Economía Social - IPES, a través del Comité de Sistemas y Seguridad de la Información debe construir, implementar, revisar y actualizar la política de seguridad.

Todo software de cómputo debe ser comprado o aprobado por el área de Sistemas en concordancia con la política de adquisición de la entidad.

El Instituto para la Economía Social - IPES debe contar con un dispositivo de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes.

Los jefes de área deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para alcanzar conformidad con las políticas de seguridad de la información.

El Instituto para la Economía Social - IPES en caso de tener un servicio de transferencia de archivos para intercambio de información no utilizará protocolos considerados obsoletos o inseguros como FTP o Telnet y utilizará protocolos de transferencia segura de archivos. Cuando el origen sea el Instituto para la Economía Social – IPES hacia entidades externas, el Instituto para la Economía Social - IPES establecerá los controles necesarios para el control de la seguridad de la información, cuando el origen de la transferencia es una entidad externa se acogerán las políticas de esa entidad, sin embargo se deben

revisar y proponer controles en concordancia con las políticas de seguridad de la información del Instituto para la Economía Social, esta revisión debe quedar documentada.

5.7.12. Política de Seguridad para las Relaciones con Proveedores.

Objetivo:

Mantener la seguridad y privacidad de los activos de información y los servicios de procesamiento de información a los cuales se les ha autorizado acceso a las partes externas denominados proveedores; o que son procesados, comunicados o dirigidos por estos.

Aplicabilidad:

La política aplica a toda la entidad. La tercerización o prestación de servicios con proveedores, generalmente incluye el mantenimiento de hardware y software, el contrato de consultores, contratistas externos y personal temporal.

Detalle de la política:

Los riesgos asociados con la tercerización de servicios o proveedores deben ser gestionados mediante un análisis de riesgos, con el fin de determinar los controles físicos o lógicos se van a implementar; de tal forma que se preserve la confidencialidad, disponibilidad e integridad de los activos de información, así como la finalidad del uso y tratamiento de los datos en los casos que aplique, de acuerdo a los procedimientos legales y administrativos, con el objeto de garantizar el adecuado manejo de la información.

Frente a la selección del proveedor o proveedora: Se deben exigir criterios de selección que contemplen la historia y reputación de la empresa, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, procesos de selección de personal, seguimiento de estándares de gestión de calidad y seguridad, se deben validar los antecedentes del proveedor o proveedora o parte interesada conforme a los procedimientos establecidos por el Instituto de Economía Social - IPES, con el objeto de garantizar el adecuado manejo de la información; y determinar otros criterios que resulten de un análisis de riesgos del proceso de selección.

Análisis de riesgos: Se deben identificar los riesgos de seguridad de la información y los servicios de procesamiento de los datos de la entidad en los procesos de negocio que involucran proveedores. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado a la Dirección antes de firmar un

contrato con el proveedor o proveedora.

Consideraciones de seguridad: Para todos los terceros que requieran tener acceso a los activos de información de la entidad, se deben definir claramente todos los requisitos de seguridad y privacidad de información internos, para que sean aplicados a los mismos, dentro de estos se encuentran: las políticas, convenios, acuerdos de niveles de servicio, la finalidad del tratamiento de la información, personal que está autorizado para el tratamiento de los datos; controles a tener en cuenta antes, durante y después del tratamiento de los datos por parte del o de la contratista, proveedor o proveedora o parte interesada, responsabilidades legales y derechos de propiedad intelectual entre otros.

Acuerdos entre las partes: Un contrato formal entre la entidad y el tercero debe existir para proteger ambas partes. El contrato definirá claramente el tipo de información que intercambiarán las partes. Si la información intercambiada no es pública, un **acuerdo de confidencialidad** entre la entidad y el tercero debe ser preparado de acuerdo al objetivo y alcance del contrato y firmado por ambas partes. En todos los casos deben firmarse acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad de la información y con los objetivos del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI y del Instituto para la Economía Social - IPES.

En caso de que se identifique una amenaza que pueda llegar a vulnerar la información, se debe reportar a la Subdirección Administrativa y Financiera y a la Subdirección de Diseño y Análisis Estratégico.

El custodio del activo de información no deberá permitir el acceso a los activos de información hasta no tener firmados y formalizados, los contratos, acuerdos o convenios con los y las proveedores, los fines de uso, condiciones de tratamiento, las cláusulas de confidencialidad; así como el debido análisis de riesgos y la implementación de los controles requeridos para preservar las características de confidencialidad, integridad y disponibilidad de la información.

5.7.13. Política de Seguridad sobre el Uso de Controles Criptográficos.

Objetivo:

Proporcionar medios criptográficos adecuados para proteger la confidencialidad, autenticidad o integridad de la información cuando sea necesario.

Aplicabilidad:

Esta política aplica para cualquier información que se maneje en el Instituto para la Economía Social IPES, la almacenada en los sistemas de información, la información transportada por los medios y dispositivos móviles o removibles o a través de las redes informáticas, y que por su clasificación requiere asegurarse por sistemas criptográficos.

Detalle de la política:

El Comité de Sistemas y Seguridad de la Información de la entidad definirá de acuerdo a la clasificación y análisis de riesgos de la información, qué datos deben ser cifrados y su nivel de protección para escoger el tipo de algoritmo criptográfico utilizado o las herramientas para el cifrado de información. La Dirección y el Comité de Sistemas y Seguridad de la Información, dará las directrices necesarias para asignar el o la responsable o responsables de la implementación del sistema criptográfico y el cómo se gestionan las claves que usa el sistema.

Conforme a los roles y responsabilidades en el tratamiento de la información será autorizado el uso de herramientas de cifrado para los funcionarios y funcionarias, contratistas o en general en el Instituto para la Economía Social - IPES.

Para la solicitar acceso o actualización al sistema o llaves de cifrado se debe elevar petición formal a la Dirección y al Comité de Sistemas y Seguridad de la Información.

Los funcionarios y funcionarias o contratistas autorizados para uso de sistemas de cifrado de datos deben conservar la disponibilidad, integridad y confidencialidad de las llaves, herramientas o algoritmos de cifrado; así como de la información a la cual se le haya aplicado este procedimiento.

Para la eliminación de la información cifrada o descifrada se implementarán las técnicas de borrado seguro.

Los funcionarios y funcionarias, contratistas o terceros tienen la responsabilidad de reportar, mediante los canales autorizados, las fallas reales o potenciales y los posibles riesgos de las herramientas de cifrado ante la Dirección y el Comité de Sistemas y Seguridad de la Información.

El Comité de Seguridad de la Información tendrá en cuenta la legislación y marcos normativos vigentes cuando se utilizan sistemas o llaves criptográficas sobre la información, en especial la ley 594 de 2000, la ley 527 de 1999 y el decreto 333 de 2014.

Para aquellos sistemas de información que en la actualidad cuentan con algún mecanismo

de cifrado deben acogerse a la presente política.

5.7.14. Política de Seguridad de Gestión de Llaves Criptográficas Objetivo:

Establecer las directrices para el uso y disposición de las Llaves Criptográficas para proteger la confidencialidad, autenticidad o integridad de la información.

Aplicabilidad:

Esta política aplica para cualquier proceso o área que haga uso de llaves criptográficas en el Instituto para la Economía Social - IPES.

Detalles de la Política:

La Subdirección de Diseño y Análisis Estratégico será el responsable de la gestión de las llaves criptográficas: creación, activación, distribución y revocación de las mismas a los usuarios y usuarias autorizadas y realizará seguimiento para que las llaves se encuentren activas en el período de tiempo previsto.

Quienes estén autorizados o autorizadas para el uso de las llaves criptográficas y/o los responsables de éstas deberán almacenarlas de forma segura, de tal forma que se limite el acceso sólo a los usuarios y usuarias autorizados, en especial cuando se ausenten de su puesto trabajo y se hayan estado utilizando. En caso de que exista una copia de las llaves, ésta se debe almacenar en un sitio seguro para su recuperación garantizando su disponibilidad en caso tal que se extravíe.

Cuando exista sospecha de que pudieron ser accedidas por una persona no autorizada, se materialice un riesgo o el funcionario o funcionaria termine su relación laboral o vínculo contractual con el Instituto para la Economía Social - IPES, las llaves serán revocadas por el o la oficial de seguridad de la información o persona delegada por el Comité de Sistemas y Seguridad de la información.

El periodo de vigencia de las llaves criptográficas del Instituto para la Economía Social – IPES, será definido por el Comité de Seguridad de la información o su delegado; en caso de llaves criptográficas expedidas por terceros serán ellos quienes definan la vigencia de las mismas.

5.7.15. Política de Seguridad para Dispositivos Móviles y Teletrabajo.

Objetivo:

Garantizar la seguridad de la información cuando se utilizan dispositivos de comunicación móvil dentro de la entidad o cuando se usan estos u otros dispositivos para realizar funciones o actividades de teletrabajo en el Instituto para la Economía Social - IPES.

Aplicabilidad:

Esta política aplica para cualquier equipo o conexión de trabajo remoto autorizada, que tenga acceso a la información ya sea almacenada o no en los sistemas de información del Instituto para la Economía Social - IPES y que por su clasificación necesita protegerse de riesgos de confidencialidad e integridad.

Detalle de la política:

El Comité de Sistemas y Seguridad de la Información del Instituto para la Economía Social – IPES, de acuerdo a la tecnología existente definirá las directrices necesarias para la aprobación de conexión de equipos de tecnología móviles tales como celulares, portátiles, tabletas y teléfonos inteligentes entre otros, a los servicios de red de la entidad.

La Dirección y el Comité de Sistemas y Seguridad de la Información de la entidad, definirán las directrices requeridas para la aprobación de actividades de teletrabajo dependiendo de las necesidades de la entidad, características de trabajo dentro o fuera de la entidad, modalidades (trabajadores con contrato laboral, trabajadores independientes, trabajadores que utilizan dispositivos móviles), beneficios y obstáculos de acuerdo a la ley 1221 de 2008 y al decreto 0884 de 2012 que reglamenta el teletrabajo en Colombia.

Los servicios de red y acceso a Internet del Instituto para la Economía Social - IPES cuentan con herramientas de control de seguridad de la información que son de estricto cumplimiento por parte de los funcionarios y funcionarias, contratistas y terceros para el acceso a la información, sistemas informáticos, aplicativos y demás; a través de cualquier dispositivo de tecnología móvil (computadores portátiles, Smartphone, tabletas, entre otros.

La conexión remota empleada para realizar teletrabajo en los sistemas de información del Instituto para la Economía Social – IPES debe ser hecha a través de una conexión VPN (Red Privada Virtual) segura suministrada por la entidad, la cual debe ser aprobada por el

Comité de Sistemas y Seguridad de la Información, registrada y auditada.

Para el acceso a la red del Instituto para la Economía Social – IPES, los visitantes solo podrán tener acceso a la información mediante redes inalámbricas diferentes a las redes de flujo de trabajo de los sistemas de información de la Entidad.

Los dispositivos móviles propiedad del Instituto para la Economía Social – IPES, se deben proteger física y lógicamente para garantizar la seguridad de la información y evitar el hurto de éste, cuando estén dentro o fuera de las instalaciones de la Entidad.

El o la custodia del dispositivo móvil es el responsable de aplicar los controles de seguridad recomendados por el Comité de Sistemas y Seguridad de la Información para la protección de la información y los dispositivos móviles.

Según los niveles de calificación de la información que se almacena en el dispositivo móvil, se determinará la necesidad del cifrado de la misma, así como la ejecución de copias de respaldo o backup.

Para el caso de extravío o hurto de un dispositivo móvil propiedad del Instituto para la Economía Social – IPES, el funcionario o funcionaria o contratista responsable del dispositivo será quien informe de manera inmediata a la Subdirección Administrativa y Financiera el suceso, con el fin de establecer las medidas de seguridad adecuadas para la protección de la información que contenga el dispositivo y acceso a los sistemas de información desde el mismo.

Los funcionarios y funcionarias o contratistas no deben instalar software en los dispositivos móviles de propiedad del Instituto para la Economía Social – IPES, sin previa autorización y coordinación con la mesa de ayuda.

Evitar en lo posible, realizar conexiones externas a redes públicas inseguras desde los dispositivos móviles que sean propiedad del Instituto para la Economía Social - IPES.

Cuando el dispositivo móvil en el que se accede a la información y sistemas del Instituto para la Economía Social - IPES haya sido extraviado o robado al funcionario o contratista responsable, la Mesa de Ayuda tiene la potestad de realizar la desactivación, borrado y retiro de los accesos a los sistemas institucionales.

Los funcionarios y funcionarias o contratistas que tengan autorización de uso de dispositivos móviles para ejecución de sus funciones, deben dar estricto cumplimiento a los siguientes lineamientos:

- Cuando se trate de dispositivos móviles propios, al llegar a las instalaciones del Instituto para la Economía Social – IPES, se deben registrar ante el personal de vigilancia indicando marca, modelo y número de serie del dispositivo; igualmente registrar la salida del equipo ante el personal de vigilancia.

- Para el caso de dispositivos móviles propiedad del Instituto para la Economía Social – IPES, se debe tramitar autorización ante la Subdirección Administrativa y Financiera, aplicando los procedimientos definidos por la entidad para el retiro de éstos, incluyendo el registro del tiempo que se autoriza la salida del equipo (fecha de salida y la fecha de devolución).

- Cuando se realice la devolución del dispositivo móvil al Instituto de la Economía Social – IPES se debe reportar a las áreas responsables, los eventos o incidentes que afectaron directa o indirectamente al equipo.

- En caso de que se requiera soporte técnico sobre el dispositivo móvil autorizado, se debe comunicar con la Mesa de Ayuda.

5.7.16. Política de Seguridad de Transferencia de Información Objetivo:

Definir las directrices para el intercambio o transferencia de información, entre funcionarios, contratistas y terceros en el Instituto para la Economía Social – IPES; o cuando se requiera entre entidades externas y terceros interesados, preservando los principios de disponibilidad, integridad y confidencialidad de la información.

Aplicabilidad:

Esta política aplica a todos los funcionarios y funcionarias y/o contratistas del Instituto para la Economía Social – IPES, cuando se trate de información pública reservada o pública clasificada, que se requiera transferir por medios digitales o físicos.

Detalle de la Política:

Los funcionarios y funcionarias, contratistas o terceros que requieran transferir externamente información sensible (pública clasificada o pública reservada), deben firmar el "**Acuerdo de confidencialidad**" donde se describan las responsabilidades de las partes y se garantice la reserva de la información; de igual forma, deben contar con la autorización previa de su jefe o jefa inmediata.

Los funcionarios y funcionarias, contratistas o terceros que requieran transferir información

para el cumplimiento de sus funciones, deben utilizar los medios, herramientas de cifrado y demás recursos aprobados y dispuestos por el Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos de la Subdirección de Diseño y Análisis Estratégico para tal fin.

Los funcionarios y funcionarias, contratistas o terceros deben implementar el procedimiento de Transferencia de Información, el cual contiene las directrices a tener en cuenta al momento de intercambiar información catalogada como pública clasificada o pública reservada.

La transferencia o intercambio de información con entes de control y autoridades de supervisión, se rige por las directrices y mecanismos que dispongan dichos entes de control y la normatividad vigente.

Se deben implementar herramientas de cifrado de información cuando se trate de información pública reservada y pública clasificada, de acuerdo a lo definido por el Comité de Sistemas y Seguridad de la Información o su delegado, en todo caso, se debe garantizar el uso de los controles establecidos por el Instituto para la Economía Social - IPES.

Sin excepción, los intercambios de información con otras entidades o partes externas interesadas, diferentes a los entes de control, deben estar soportados por medio de contratos, convenios o acuerdos formalizados, en donde se determinarán los medios y controles para el tratamiento de la información. De igual forma, se deben firmar acuerdos de confidencialidad que garanticen la protección de la información durante y después del tiempo de ejecución de los compromisos, cumpliendo la normatividad vigente en materia de protección de datos, especialmente la relativa a la Ley de Habeas Data (Ley 1266 de 2008 y sus decretos reglamentarios), la Ley de Protección de Datos Personales (Ley 1581 de 2012 y decretos reglamentarios) y Ley de Transparencia (Ley 1712 de 2014 y sus decretos reglamentarios).

Para la transferencia de información se deben analizar y tratar los riesgos relativos al uso de la información y la utilización de los diferentes canales de comunicación, de forma que se mantengan en los niveles de seguridad aceptables del Instituto para la Economía Social - IPES. En cualquier medio que se lleve a cabo la transferencia de información (física o electrónica), se debe dar el cumplimiento a las políticas y procedimientos de seguridad de la información, de tal forma que se preserven los niveles de confidencialidad e integridad de los datos contenidos o transferidos.

5.7.17. Política de Seguridad de Desarrollo Seguro Objetivo:

Establecer y aplicar los requisitos de Seguridad de la Información en el Instituto para la Economía Social - IPES, para el desarrollo de software como parte de todo el ciclo de vida del sistema.

Aplicabilidad:

Esta política aplica para todo el software que sea desarrollado para la entidad; incluye el desarrollo In House como el desarrollo realizado por terceros.

Detalle de la Política:

Se deben identificar, acordar, justificar y documentar los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo de software.

Se deben incluir puntos de control de seguridad dentro de las fases del ciclo de vida de desarrollo de software.

Todo cambio, modificación o versión en el ambiente de producción debe contar con controles de seguridad, para evitar pérdida de información en caso de que deba darse marcha atrás; entre ellos, realizar una copia de respaldo para mantener la integridad de los datos y de los sistemas de información, y documentar los cambios realizados.

Los ambientes de desarrollo, pruebas y producción, deben estar separados.

En el ambiente de pruebas se deben realizar pruebas de seguridad, con el fin de identificar vulnerabilidades, y resolver los inconvenientes antes del paso a producción.

Los usuarios y usuarias y/o terceros que están involucrados en cada fase, deben utilizar perfiles diferentes en cada ambiente (Desarrollo, pruebas y producción); además, asegurar que cada usuario y usuaria cuente únicamente con los privilegios necesarios que se requieren en cada ambiente.

El ambiente de prueba debe simular el ambiente de producción. Sin embargo, los datos de prueba utilizados, a pesar de corresponder a una estructura igual o similar a la de producción, deben utilizarse técnicas de enmascaramiento (ofuscación), para garantizar la seguridad y protección de los datos.

En caso de requerirse información para el ambiente de pruebas, se debe validar que la información entregada a los desarrolladores para la ejecución de las mismas se encuentre

enmascarada o que los datos sensibles son eliminados con el fin de no revelar información confidencial de los ambientes de producción y, por ende, dar cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y a la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública).

Se deben aplicar los mismos controles del ambiente de producción en el ambiente de desarrollo, como lo son: control de acceso, copias de respaldo, registro de eventos.

El Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos de la Subdirección de Diseño y Análisis Estratégico debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y producción han sido aprobadas.

La Subdirección de Diseño y Análisis Estratégico debe contar con un procedimiento para control de versiones con el fin de administrar los cambios en los sistemas de información desarrollados al interior del Instituto para la Economía Social – IPES.

En caso de contratar desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por el Instituto para la Economía Social - IPES. Adicionalmente, se debe acordar la entrega de manual(es) técnico(s), que describen la estructura interna del sistema, así como el diccionario de datos, librerías y archivos que lo conforman; y manual(es) funcional(es), que describen las funcionalidades de cada una de las opciones del menú de la aplicación.

La Subdirección de Diseño y Análisis Estratégico a través de su delegado o delegada debe asegurar que los sistemas de información adquiridos o desarrollados por terceros cuenten con las respectivas licencias y se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.

5.7.18. Políticas de empleo de Sistemas de Información Objetivo:

Reglamentar el uso de los sistemas de información provistos por el IPES, para garantizar adecuadas fuentes de información, trazabilidad al quehacer misional y la adecuada protección de la información de la entidad.

Aplicabilidad:

Estas políticas aplican a todos los usuarios y usuarias de los sistemas del Instituto para la Economía Social actuales o por ingresar.

Detalle de la Política:

El proceso de gestión de seguridad de la información y recursos tecnológicos es responsable por la disponibilidad de los sistemas de información críticos de la entidad y herramientas principales de apoyo en la toma de decisiones de la Dirección.

Cada dependencia, área o subdirección al interior del Instituto para la Economía Social - IPES, será encargada de implementar las políticas de seguridad de la información de las aplicaciones que administre sea con recurso propio o a través de un tercero conservando la integridad de la información y bajo políticas de confidencialidad, no obstante se apoyará de la asesoría técnica y herramientas transversales con las que cuenta la Subdirección de Diseño y Análisis Estratégico (SDAE).

Los usuarios y usuarias de los sistemas de la entidad, no podrán desarrollar ninguna herramienta paralela para el tratamiento de actividades administrativas y misionales diferentes a las que le provee el IPES.

La información consignada en los sistemas de información del IPES es legalmente del Instituto, no del personal a cargo del registro de información o empresas tercerizadas de software que alquilen o provean el sistema/producto y solo puede emplearse con la finalidad del cumplimiento misional y control administrativo.

El uso indebido de la información de la entidad, o la negativa a emplear los sistemas de Información que ha dispuesto serán sujeto de las acciones disciplinarias o legales dispuestas por el Instituto para la Economía Social - IPES.

El Instituto para la Economía Social se reserva el derecho de proteger su información promoviendo controles internos para prevenir el uso indebido, las copias no autorizadas y la distribución de la información. Estos controles pueden incluir auditorías anunciadas y no anunciadas, registro de actividades de los usuarios y usuarias de los sistemas de información.

Los usuarios y usuarias, independiente de la modalidad de vinculación y en el marco de sus obligaciones contractuales en el caso que corresponda, deben hacer uso de los sistemas de información suministrados por la entidad con el fin de registrar, consolidar, identificar, caracterizar, focalizar, las actuaciones administrativas y misionales del Instituto para la Economía Social.

Los usuarios y usuarias sólo tendrán acceso a los datos y recursos autorizados por el

Instituto para la Economía Social - IPES, y serán responsables por la divulgación no autorizada de esta información.

Cualquier incidente o posible evento que afecte la seguridad de la información debe ser reportado inmediatamente a la jefatura de área o a la mesa de ayuda o al área designada para este fin.

El personal de la entidad debe ser consciente que debe tomar las precauciones necesarias para no revelar información considerada como clasificada o reservada, cuando se hace una llamada telefónica que puede ser interceptada mediante acceso físico a la línea o al auricular o escuchada por personas que se encuentren cerca. Lo anterior, debe aplicar también cuando el empleado se encuentre en sitios públicos como restaurantes, transporte público o ascensores.

Así mismo, las credenciales de acceso a recursos como la VPN y los sistemas de información de la entidad son de uso exclusivo del usuario o usuaria, no deben ser compartidos y deben ser tratados con la responsabilidad que enmarca esta política.

5.7.19. Política Derechos de propiedad intelectual Objetivo:

Establecer los lineamientos necesarios para verificar y asegurar el cumplimiento de los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual.

Aplicabilidad:

Estas políticas aplican a todo el Instituto para la Economía Social – IPES, comprendiendo funcionarios, funcionarias, contratistas, terceros directivas y personal administrativo, que realizan labores regulares propias de la actividad laboral y contractual, que generen conocimiento, desarrollo, creación, obras o productos susceptibles de ser protegidos por propiedad intelectual en cualquiera de sus modalidades, ya sea por alianzas, o convenios.

Detalle de la Política:

Todo software o productos informáticos que utilice el Instituto para la Economía Social actuales – IPES deben cumplir con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual en los aspectos relacionados con su divulgación y difusión.

A continuación se detallan los lineamientos para el cumplimiento de los requisitos

legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual.

- El Proceso de Gestión Seguridad Información y Recursos Tecnológicos realizará revisiones periódicas a través del funcionario o funcionaria designada para tal fin (al menos una vez al año), con el fin de asegurar que todo el software que se ejecute en la Entidad esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

- Los usuarios y usuarias no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos portátiles suministrados por la entidad para el desarrollo de sus funciones.

- Los usuarios y usuarias deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, El proceso de Gestión Seguridad Información y Recursos Tecnológicos podrá distribuir un número de copias de software bajo una licencia otorgada.

  Ley 23 de 1982: Por la cual se regula los derechos morales y patrimoniales que la Ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística o científica, esté publicada o inédita.
  Ley 1915 de 2018: por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derechos de autor y derechos conexos.

- Los supervisores de contratos deben asegurarse de incluir cláusulas de propiedad intelectual y derechos de autor en contratos con terceros.

5.8. COMUNICACIÓN

El Instituto cuenta con la Oficina Asesora de Comunicaciones (OAC), a través de la cual se socializan y difunden los diferentes componentes del Sistema, entre ellos el Manual del Sistema de Gestión y políticas de seguridad de la información, los protocolos, guías que lo soportan y demás los elementos necesarios para la sensibilización de los funcionarios y funcionarias y colaboradores de la Entidad.

Por lo tanto, se deben realizar las coordinaciones necesarias con la OAC para la comunicación de los temas relacionados con el Sistema de Gestión de Seguridad de la Información.

5.9. INCIDENTES DE SEGURIDAD

La entidad establece, a través del procedimiento, los métodos estándar para identificar, realizar seguimiento y responder a los incidentes de seguridad de la información que se puedan presentar al interior de la entidad. Se ha definido el siguiente procedimiento, instructivo y formatos:

- PA03-PD-002 GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- PA03-IN-002 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- PA03-FO-006 LECCIONES APRENDIDAS RESPUESTA A INCIDENTES
- PA03-FO-007 DOCUMENTACIÓN DE REPORTES/EVENTOS/INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- PA03-FO- 034 REGISTRO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

5.10. LEVANTAMIENTO DE INFORMACIÓN FORENSE

La entidad establece, a través del procedimiento, los lineamientos para contar con capacidades para realizar análisis de información forense para poder determinar qué incidentes han ocurrido sobre los sistemas de información y servicios, así como orientar en el manejo de la evidencia forense digital y su integración con la gestión de incidentes de seguridad de la información. Se ha definido el siguiente instructivo:

- PA03-IN-005 MANEJO DE INFORMACIÓN FORENSE

5.11. GESTIÓN DE LA CONTINUIDAD

Es responsabilidad de la Subdirección de Diseño y Análisis Estratégico, a través del Proceso de Gestión de la Seguridad de la Información y Recursos Tecnológicos en el establecimiento, operación, seguimiento y mejora del plan de contingencia informático.

El Comité de Sistemas y Seguridad de la Información es responsable de gestionar los recursos necesarios para definir, implementar, mantener y mejorar un plan de continuidad de la operación informática, que garantice la protección de los activos de información críticos para el instituto para la Economía Social - IPES.

El Comité de Sistemas y Seguridad de la Información es responsable de la validación de

la existencia del Plan de Contingencia Informático o Plan de Continuidad del Negocio, que garantice la recuperación de la operación informática frente a la posible materialización de riesgos de seguridad de la información, y realizará una actualización anual, en desarrollo de las acciones del plan de acción del comité.

La SDAE es responsable de la operación del plan de contingencia informático o Plan de Continuidad del Negocio, así como de la revisión de los anexos que lo conforman. Es responsabilidad de los equipos funcionales garantizar la completitud de los documentos que soportan la operación informática de la entidad.

El equipo de sistemas es responsable de la programación de los simulacros de restauración de los sistemas y servicios informáticos, según lo estipulado en el plan de contingencia. Los simulacros de restauración deben ser debidamente documentados y revisados para medir la efectividad de los componentes del plan.

El equipo de sistemas debe realizar una revisión, y de ser necesario, actualizar trimestralmente el mapa de riesgos del proceso de gestión de seguridad de la información y recursos tecnológicos de acuerdo al resultado de los simulacros o el análisis de los eventos presentados.

5.12. SEGUIMIENTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

El seguimiento al SGSI se realiza en cumplimiento de la normatividad vigente, las disposiciones legales Nacionales y Distritales, los lineamientos y directrices definidas en la NTC ISO 27001-2013 y la resolución 615 de 2013 por la cual se conforma el comité de seguridad de la información. De esta manera los usuarios y usuarias de los sistemas y servicios informáticos del IPES, tienen la posibilidad de contar con un marco de referencia que evite incurrir en conductas que originen faltas a la seguridad de la información.

La Subdirección de Diseño y Análisis Estratégico es la encargada de liderar fortalecer y hacer seguimiento al Sistema de gestión de Seguridad de la información (SGSI), pero es obligación de todos los funcionarios y funcionarias, servidores y servidoras públicas, contratistas y terceros con acceso autorizado a los servicios y sistemas informáticos, cumplir con todas las políticas y disposiciones de seguridad digital adoptadas por la entidad.

6. DOCUMENTOS ASOCIADOS

- PA03-NG-001 NORMOGRAMA PROCESO DE GESTIÓN DE LA INFORMACIÓN Y GESTIÓN DE RECURSOS TECNOLÓGICOS
- PA03-MG-001 MATRIZ DE RIESGOS GESTIÓN DE LA INFORMACIÓN Y LOS RECURSOS TECNOLÓGICOS
- PA03-IN-002 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- PA03-PD-003 - PROCEDIMIENTO CONTROL DE CAMBIOS
- PA08 DE 003 V5 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- PA03-DE-004 V4 PLAN CONTINGENCIA TI
- PA03-FO-010 V2 ACUERDO DE CONFIDENCIALIDAD

7. MARCO NORMATIVO

- Ley **1712 de 2014** de transparencia y acceso a la información pública.
- Ley **1581 de 2012**, Protección de Datos Personales los deberes y responsabilidades de los responsables y/o encargados del tratamiento de los datos personales.
- Ley **23 de 1982**, Por la cual se regula los derechos morales y patrimoniales que la Ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística o científica, esté publicada o inédita.
- Ley **1915 de 2018**, por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derechos de autor y derechos conexos.
- Ley **1266 de 2008**, Ley de Habeas Data y sus decretos reglamentarios.
- Ley **1221 de 2008** y al decreto 0884 de 2012: Que reglamenta el teletrabajo en Colombia.
- Ley **594 de 2000**, la ley 527 de 1999 y el decreto 333 de 2014: cuando se utilizan sistemas o llaves criptográficas sobre la información.
- Ley **1273 de 2009**, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"
- Ley **734 de 2002**: Por la cual se expide el Código Disciplinario Único.
- Resolución 020 de 2021, Por la cual se actualiza el Plan de Seguridad y privacidad de la información, el Plan Estratégico de Riesgos de Seguridad y Privacidad de la

Información del Instituto para la Economía Social - IPES.

- NTC-ISO/IEC 27001, Requisitos de Gestión de la Seguridad de la Información y Mapas de Aplicabilidad SOA.
- NTC-ISO/IEC 27002, Código de Práctica para los Controles de Seguridad de la Información
- Decreto 1499 de 2017, modifica el Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- PA03-NG-001 NORMOGRAMA PROCESO DE GESTIÓN DE LA INFORMACIÓN Y GESTIÓN DE RECURSOS TECNOLÓGICOS
- DECLARACIÓN DE APLICABILIDAD

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO
1	13/06/2014	-	Creación del documento

2	**17/08/2018**	Objetivo Alcance Definiciones Marco Normativo Política General Principios que soportan el desarrollo de la política Roles y Responsabilidades	Se realizó revisión integral del documento. Se cambia el nombre del documento. Se ajusta la política general del Sistema de gestión de seguridad de la información. Se incluye el numeral Marco Normativo Se incluye el numeral de Definiciones. Se incluyen roles y responsabilidades de seguridad de la información. Se eliminan los numerales del manual, que son documentos complementarios.
3	**18/05/2021**	Ajuste de Políticas Complementarias, Roles y Responsabilidades, Metodología de Riesgos y Normograma, Adición de Política y Derechos de propiedad intelectual.	Ajuste a Ítem 4 Marco Normativo Ajuste del Ítem 8 Roles y Responsabilidades de la Información Ajuste del ítem 10 Metodología de Valoración de Riesgos Ajuste a Políticas Complementarias: 12.3, 12.3.1; 12.3.2, 12.4, 12.5, 12.10, 12.11, 12.11.1, 12.12, 12.13 y 12.14 Adición del numeral 12.16. Política Derechos de propiedad intelectual

4	**20/10/2022**	Ajuste de Políticas. Políticas Complementarias del SGSI	Se realizó revisión integral del documento Ajuste a Políticas Complementarias del SGSI 5.7.1. Política de uso de Correo Electrónico, 5.7.2. Política de uso de Internet, 5.7.3. Política de Seguridad de Control de Acceso, 5.7.4. Política de Seguridad de Control de Acceso Lógico 5.7.5. Política de Seguridad de Control de Acceso Físico 5.7.6. Política de Seguridad de Escritorio y Pantalla Limpia 5.7.7. Política de Seguridad de Copias de Respaldo y Restauración 5.7.8. Política Específica de Usuario 5.7.9. Política Específica de Personal de Tecnología 5.7.10. Política de Gestión de Incidentes de Seguridad de la Información 5.7.12. Política de Seguridad para las Relaciones con Proveedores 5.7.15. Política de Seguridad para Dispositivos Móviles y Teletrabajo 5.7.16. Política de Seguridad de trasferencia de Información 5.7.17. Política de Seguridad de Desarrollo Seguro 5.7.18. Políticas de Empleo de Sistemas de la Información

5	**29/12/2023**	Ajuste de Políticas. Políticas Complementarias del SGSI	Se realizó revisión integral del documento Ajuste a Políticas Complementarias del SGSI 5.7.1. Política de uso de Correo Electrónico, 5.7.2. Política de uso de Internet, 5.7.11. Política de Seguridad de Control de Acceso, 5.7.12. Política de Seguridad de Control de Acceso Lógico 5.7.13. Política de Seguridad de Control de Acceso Físico 5.7.14. Política de Seguridad de Escritorio y Pantalla Limpia 5.7.15. Política de Seguridad de Copias de Respaldo y Restauración 5.7.16. Política Específica de Usuario 5.7.17. Política Específica de Personal de Tecnología 5.7.18. Política de Gestión de Incidentes de Seguridad de la Información 5.7.12. Política de Seguridad para las Relaciones con Proveedores 5.7.19. Política de Seguridad para Dispositivos Móviles y Teletrabajo 5.7.20. Política de Seguridad de trasferencia de Información 5.7.21. Política de Seguridad de Desarrollo Seguro 5.7.22. Políticas de Empleo de Sistemas de la Información

		Ajuste de Políticas Complementarias, Roles y Responsabilidades, Metodología de Riesgos y Normograma, Adición de Política y Derechos de propiedad intelectual.	Se ajusta todo el documento