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

IPES

MANUAL DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO

Bogotá 2018

Elaboró:	Revisó:	Aprobó:
Yamel Orlando Martínez Balaguera - CPS 60/2018 John Jair Garzón Delgado Profesional Especializado SDAE Estefanía Duque Rincón CPS 369/2018 Sandra Bibiana Carmona Profesional Universitario – SJC Myriam Stella Forero Profesional Universitario- SAF Nohora Milén Cortés Cantor – CPS 399/2018 Manuel Andrés Vivas Profesional Especializado - SDAE	Vivian Lilibeth Bernal Izquierdo – Subdirectora Administrativa y Financiera Patricia del Rosario Lozano Triviño – Subdirectora Jurídica y de Contratación Adriana Villamizar Navarro – Subdirectora de Emprendimiento, Servicios Empresariales y de Comercialización Esperanza del Carmen Sáchica de Daza – Subdirectora de Formación y Empleabilidad Hernán Carrasquilla Coral – Subdirector de Gestión, Redes Sociales e Informalidad	Clarisa Díaz García – Subdirectora de 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

El presente Manual se aplicará a los activos de información de la Entidad, por parte de todos los servidores públicos de la Entidad.

3 DEFINICIONES[1]

a. **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.

b. **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.

c. **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.

d. **Política:** toda intención y directriz expresada formalmente por la dirección.

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

f. **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.

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

h. **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)

i. **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.

j. **Sistema de Gestión de Seguridad de la Información – SGSI:** parte del sistema de gestión global, basada 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.

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

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

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

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

o. **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]

p. **Usuarios:** Funcionarios, contratistas y terceros que tienen acceso a los sistemas de información, servicios de red y a la infraestructura tecnológica que los soporta.

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

4 MARCO NORMATIVO

1. CLASIFICACIÓN NORMATIVA	2. NÚMERO DE LA NORMATIVIDAD	3. EMITE	4. AÑO	5. EPIGRAFE
Decreto	1499	Presidencia de la República	2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
Decreto	103	Presidencia de la República	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Resolución	184	IPES	2014	Por la Cual se adopta el manual del Subsistema de Gestión de Seguridad de la Información y el Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Instituto para la Economía Social - IPES
Ley	1712	Congreso de la República	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto	2573	Presidencia de la República	2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Resolución	615	IPES	2013	Por la cual se conforma el comité de Sistemas y Seguridad de la Información del Instituto para la Economía Social - IPES y se definen sus funciones
Norma	NTC-ISO-27001	International Organization for Standardization Comisión International Electrotechnical	2013	Norma elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la

		Commission.		información.
Ley	1581	Congreso de la República	2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Norma	NTDSIG001	Alcaldía de Bogotá	2011	Norma técnica Distrital del sistema Integrado de gestión para las entidades y organismos Distritales.
Directiva	22	IPES	2011	Estandarización de la información de identificación, caracterización, ubicación y contacto de los ciudadanos y ciudadanas que capturan las entidades del Distrito Capital.
Ley	1273	Congreso de la República	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
Ley	1266	Congreso de la República	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones
Resolución	305	Comisión Distrital de Sistemas	2008	Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

Decreto	619	Alcaldía de Bogotá	2007	Se establece la estrategia de gobierno electrónico de los organismos y de las entidades de Bogotá, distrito capital y se dictan otras disposiciones
Acuerdo	279	Concejo de Bogotá	2007	Por el cual se dictan los lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital.
Directiva	5	Alcaldía de Bogotá	2005	Por medio de la cual se adoptan las políticas generales de tecnología de información y comunicaciones aplicables al Distrito Capital.

5 POLITICA 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 encaminadas al cumplimiento de su misionalidad, se compromete a definir, implementar, mantener y mejorar un sistema de gestión de seguridad de la información que le permita contar con niveles apropiados de integridad, confidencialidad y disponibilidad de sus activos de información, en el marco del cumplimiento de las leyes, decretos, normas y lineamientos del orden Distrital y Nacional.

El Instituto para la Economía Social gestionará, a través del Comité Institucional de Gestión y Desempeño, los recursos necesarios para minimizar el impacto sobre los activos de información, a partir de una adecuada gestión de riesgo, promoviendo el compromiso y participación del talento humano y la mejora continua para apropiar una cultura de seguridad de la información en el marco de su misión y objetivos institucionales.

Es obligación de todos los funcionarios, 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

5.1. Principios que soportan el desarrollo de la Política de Seguridad y Privacidad de la Información.

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

2. La información derivada del uso de los sistemas y servicios informáticos del Instituto para la Economía Social (sistema de información misional y administrativo, plataforma de correo Electrónico Institucional, file server) 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.

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

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

5. El Instituto para la Economía Social 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 perdida de activos de información institucional.

6. El Instituto para la Economía Social desarrolla el Subsistema 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.

7. El Instituto para la Economía Social 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 consolidan la población objeto de atención.

8. El Instituto para la Economía Social 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 la directrices de usabilidad, accesibilidad, transparencia, control, conservación, guarda y custodia de los activos de información institucional digital.

6 OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

- Establecer lineamientos, directrices, controles y en general la intención de la Dirección del Instituto para la Economía Social de consolidar el uso apropiado de los servicios de procesamiento de información, que permitan la protección de los activos de información institucional.

- Definir la responsabilidad en la definición, operación, seguimiento y mejora de las políticas institucionales relacionadas con la seguridad de la información en la entidad, al Comité Sistemas y Seguridad de la Información.

- Orientar a los funcionarios, contratistas y terceros sobre la responsabilidad de uso y buen manejo de los activos de información y de la infraestructura tecnológica que soporta la operación informática de la entidad.

- Definir aspectos a ser tenidos en cuenta por la entidad, relacionados con el talento humano y su responsabilidad en el uso de la información institucional antes, durante y en la terminación del vínculo laboral.

- Establecer directrices para la protección física de los activos de infraestructura tecnológica de la entidad.

- Establecer responsabilidades, controles y lineamientos en procura de proteger los sistemas y servicios informáticos por medio de los cuales se procesa la información institucional, que garanticen la operación informática de la entidad.

- Fomentar la conciencia alrededor de la importancia en el aseguramiento de la información institucional, la cual debe ser adoptada como una cultura organizacional.

7 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 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.

La 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), 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 para el cumplimiento de sus funciones.

8 ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACION

La implementación del Modelo de Seguridad y Privacidad de la Información, en desarrollo de las actividades del Subsistema de Gestión de Seguridad de la Información en el Instituto para la Economía Social – IPES, requiere de un componente fundamental para 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 reglamenta 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.

8.1 Comité de Sistemas y Seguridad de la Información - CSSI

Es responsabilidad del CSSI, asegurar el apoyo de la Dirección General, para soportar la administración y desarrollo de directrices asociadas a la seguridad y privacidad de la información en la entidad, a través del establecimiento y control de roles y responsabilidades, en el marco de la formulación e implementación de la política de seguridad de la información.

Se establece la responsabilidad en el aseguramiento, guarda y custodia de la información digital, derivada del uso de los sistemas y servicios informáticos misionales y administrativos, a la Subdirección de Diseño y Análisis Estratégico, proceso de gestión de seguridad de la información y recursos tecnológicos.

8.2 Oficial de Seguridad de la Información

El comité de sistemas y seguridad de la información, designará al oficial de seguridad de la información, el cual tiene como obligaciones principales:

- Liderar el diseño de políticas, directrices y lineamientos encaminados a fortalecer la seguridad de la información.

- Identificar el grado de madurez en la implementación del Modelo de seguridad y privacidad de la información en la entidad.

- Socializar ante el comité de sistemas y seguridad de la información, los incidentes de seguridad de la información presentados, así como las acciones tomadas para reducir su impacto.

- Coordinar las actividades correspondientes a la gestión de incidentes de seguridad, con la finalidad de contar con un enfoque estructurado y planificado que permita manejar adecuadamente los incidentes de seguridad de la información.

- Establecer estrategias de defensa proactivas y reactivas.

- Consolidar los procedimientos de seguridad informática y someterlos a decisión del comité de sistemas y seguridad de la información.

- Desarrollar, mantener y comunicar las políticas, estándares y guías de seguridad de la información, especialmente, aquellas con un enfoque tecnológico.

- Coordinador el análisis de riesgos de seguridad de la información y coordinar el plan para la mitigación de los mismos.

- Elaborar o coordinar campañas de sensibilización.

- Realizar capacitación y socialización del SGSI.

El rol de Oficial de Seguridad de la Información, será asumido por el/la Subdirector (a) de Diseño y Análisis Estratégico, hasta tanto el comité haga oficial la designación del responsable a través de los medios dispuestos por la entidad.

8.3 Responsable del tratamiento de la información

En cumplimiento de los lineamientos establecidos en la ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”, se define el rol de responsable del tratamiento de la información a la Subdirección de Diseño y Análisis Estratégico.

“e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;

g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.”

Teniendo en cuenta que el responsable del tratamiento de datos personales en la entidad, es quien tiene decisión sobre las bases de datos que contengan este tipo de datos y que el responsable es quien direcciona las actividades de los encargados de los datos personales (quien realiza el tratamiento directamente), como se mencionaba anteriormente, adicional a las responsabilidades arriba citadas se tendrán en cuenta que de acuerdo a la Ley 1581 de 2012 Protección de Datos Personales los deberes y

responsabilidades de los responsables y/o encargados del tratamiento de los datos personales son:[3]

- Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
- Tramitar las consultas, solicitudes y reclamos.
- Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.
- Respetar las condiciones de seguridad y privacidad de información del titular.

8.4 Nivel Directivo

El/la Director/a, Subdirectores/as y Jefes de Oficina, establecerán la necesidad del uso de la funcionalidad (rol) de los servicios y sistemas informáticos de la entidad, autorizando a los funcionarios, contratistas y terceros qué, según la naturaleza de sus funciones o competencias, requieran tener acceso a la información institucional, informando oportunamente a la Subdirección de Diseño y Análisis Estratégico a través del documento institucional vigente (Formatos Gestión de Usuarios).

Revisar y aprobar las iniciativas relacionadas con la capacitación, socialización, sensibilización y divulgación de los lineamientos y directrices relacionadas con la seguridad de la información en la entidad.

8.5 Subdirección Administrativa y Financiera – Talento Humano

Apoyar la realización de iniciativas relacionadas con la capacitación, socialización, sensibilización y divulgación de los lineamientos y directrices relacionadas con la seguridad de la información en la entidad.

Informar al proceso de gestión de seguridad de la información y recursos tecnológicos, las novedades (vacaciones, incapacidades, retiros) relacionadas con el recurso humano de la entidad.

8.6 Subdirección Administrativa y Financiera – Gestión Documental

Apoyar la identificación y clasificación de los activos de información institucional en atención a la normatividad Nacional y Distrital relacionada con el uso, acceso, protección y conservación de la información, y hacer seguimiento a la aplicación de los documentos institucionales que soportan la gestión documental en la entidad.

[3] Ministerio de Tecnologías de la Información y las Comunicaciones – Roles y Responsabilidades Seguridad y Privacidad de la Información – 2016. 6.3.2 Equipo del Proyecto, Pág. 15, 16, 17.

8.7 Asesoría de Control Interno

La entidad debe llevar a acabo auditorías internas del SGSI a intervalos planificados, para determinar si los objetivos de control, controles, procesos y procedimientos del SGSI. Se ha definido el siguiente procedimiento:

- Procedimiento de Auditorías internas PR-001

8.8 Oficina Asesora de Comunicaciones

Participar en la definición y ejecución de estrategias de comunicación de los lineamientos, directrices y controles de seguridad y privacidad de la información.

Mantener niveles apropiados de disponibilidad del sitio web institucional, así como de los activos de información susceptibles de publicaciones, en el marco de la ley 1712 de 2014 de transparencia y acceso a la información pública.

8.9 Subdirección de Diseño y Análisis Estratégico - Sistema Integrado de Gestión

Controlar los componentes documentales que consolidan el Subsistema de Gestión de Seguridad de la Información en el marco del Modelo de Seguridad y Privacidad de la información – MSPI y Modelo Integrado de Planeación y gestión – MIPG.

Realizar acompañamiento en la armonización de los componentes del subsistema en consideración a los lineamientos del modelo integrado de planeación y gestión – MIPG y demás normatividad vigente con la el Subsistema de Seguridad de la información,

Administrar y gestionar la documentación asociada al sistema integrado de gestión, en aspectos fundamentales de disponibilidad e integridad.

8.10 Subdirección de Diseño y Análisis Estratégico – Proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos

Implementar, mantener y mejorar controles de seguridad informática para contar con niveles apropiados de integridad, confidencialidad y disponibilidad de la información.

Liderar la formulación e implementación de políticas, lineamientos y directrices de seguridad y privacidad de la información.

8.11 Subdirecciones Misionales

Dar estricto cumplimiento a los lineamientos, directrices y controles de seguridad y privacidad de la información, implementados por la entidad, en el uso apropiado de los activos de información institucional, sistemas de información, servicios de red, infraestructura tecnológica.

Aplicar controles de acceso a la información recolectada en desarrollo de las actividades misionales de identificación y caracterización de la población objeto de atención, en cumplimiento de la política de tratamiento de datos personales implementada por la entidad y de la normatividad relacionada con el uso de datos personales.

8.12 Usuarios de los sistemas y servicios informáticos

Los funcionarios, contratistas y terceros con acceso autorizado al uso de los servicios y/o sistemas informáticos, deben cumplir con todas las políticas sobre el acceso y uso de información institucional, emitidas por la entidad y demás disposiciones legales vigentes, cláusulas contractuales y acuerdos de confidencialidad, so pena de investigación disciplinaria, civil y/o penal.

Los usuarios del sistema, tienen la responsabilidad de actualizarse en temas relacionados con la gestión de la seguridad de la información definidos y socializados a través del Comité Sistemas y Seguridad de la Información.

Los usuarios deben mantener la confidencialidad sobre la información del Instituto para la Economía Social, durante el vínculo con la entidad.

Los usuarios deben mantener la confidencialidad sobre la información del Instituto para la Economía Social, una vez terminado el vínculo con la entidad.

Los usuarios del sistema son responsables de informar oportunamente al proceso de gestión de seguridad de la información y recursos tecnológicos., sobre situaciones que puedan comprometer la seguridad de la información, haciendo uso de la metodología para la gestión de incidentes de seguridad de la información.

9 GESTION DE ACTIVOS

9.1. Propiedad Intelectual

La información creada, procesada o modificada haciendo uso de los sistemas y servicios informáticos proporcionados por la IPES a los usuarios 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.

9.2. 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 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, incluirá cláusulas de confidencialidad de la información institucional, en los contratos de prestación de servicios, en desarrollo de los procesos de selección. Los usuarios que ingresan a la entidad que 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.

9.3. 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, 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 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 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 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 (SIAFI) y de gestión.

- **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).

- **Backup de Usuario:** La ejecución de tareas de backup de la información contenida en los equipos de cómputo es responsabilidad de los usuarios; el equipo de sistemas realiza tareas de acompañamiento en la forma en cómo se pueden hacer las copias de seguridad.

10 METODOLOGIA DE VALORACION 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 subsistema 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.

Una descripción detallada de esta metodología se encuentra en el Instructivo de Identificación de Riesgos de Seguridad IT.

10.1. Análisis de Riesgos

- **Identificar los activos que apoyan el proceso seleccionado:** Se considera como activo cualquier cosa que tiene valor para la entidad, se debe tener en cuenta que los procesos se apoyan en sistemas de información que además de software y hardware también están compuestos por documentos (registros, instrucciones de trabajo, procedimientos), personas (responsables de actividades en el proceso o administradores de infraestructura tecnológica) y directrices que guían el proceso en sí mismo.

- **Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas:** Se considera como vulnerabilidad una debilidad en un activo o un control que puede ser explotada (aprovechada) por una amenaza.

- **Identificar las amenazas que pueden afectar a los activos:** Se considera como amenaza (causa), cualquier agente externo al activo que puede aprovechar una vulnerabilidad del mismo para causar daño y que afectará la seguridad de la información.

- **Identificar los Eventos:** Los eventos son las situaciones que se generan a partir de la combinación de una amenaza y una vulnerabilidad.

- **Identificar los Impactos:** Los impactos son los hechos que se derivan del evento identificado. A nivel de los riesgos de la seguridad de la información, los impactos se describen en términos de la pérdida de la Disponibilidad, la Integridad o Confidencialidad.

- **Identificación de controles existentes:** Se considera como control un proceso, política, dispositivo, practica u otra acción existente que actúa para minimizar el riesgo negativo o potenciar oportunidades positivas.

- **Calcular el valor del activo:** El valor del activo se calcula de acuerdo a su valoración frente a la confidencialidad, integridad y disponibilidad.

- **Calcular el valor de la posibilidad de ocurrencia (probabilidad):** El cálculo de la probabilidad de ocurrencia se realiza de acuerdo a una estimación cuantitativa.

- **Estimar los niveles de riesgo:** Asignar un valor de estimación a un impacto y probabilidad de un riesgo.

10.2. Evaluación de Riesgos

- **Priorización de riesgos y cálculo del riesgo residual:** Una vez estimados los niveles de riesgo, se deben ordenar y priorizar de manera exhaustiva, con el objetivo de formular el plan de tratamiento del riesgo de manera ordenada, es decir empezar por los riesgos extremos teniendo en cuenta su impacto.

  Para cada riesgo verificamos si hay un control existente que lo pueda mitigar o si es necesario fortalecer y mantener dicho control, o por el contrario, definir e implementar uno nuevo, con el fin de reducir la estimación del riesgo. Luego de la aplicación del control se recalcula el nuevo valor del riesgo, que es equivalente al riesgo residual. Cuando existe un control, se verifica si este es de tipo preventivo o correctivo, si se aplica, si es efectivo, si está documentado y si disminuye el impacto o la probabilidad del riesgo. Si el control existente no se aplica o no es efectivo el riesgo inicial será igual al riesgo residual.

11 DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad, es un documento clave e importante para el subsistema 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-IEC27001.

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.

12 POLÍTICAS COMPLEMENTARIAS DEL SGSI

12.1. Política de uso de correo electrónico

Objetivo:

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

Principios y Aplicabilidad:

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

Los usuarios autorizados para usar el servicio de correo electrónico 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 debe ser autorizada por el/la Directora/a, Jefes de Oficina, y Subdirectores/as a la cual pertenezca cada usuario, a través del formato institucional vigente. Dicho formato valida la asignación de perfiles y/o roles que el usuario desarrollará en la entidad. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desempeñada y no debe utilizarse para ningún otro fin.

Las contraseñas de los correos electrónicos institucionales se encontraran sincronizadas con el Directorio Activo, es responsabilidad de los usuarios mantener su contraseña de forma segura y no revelarla ya que la misma es personal e intransferible.

Los funcionarios, 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 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 es responsable de informar de contenidos o acceso 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 contratistas a quienes se haya asignado una cuenta de correo institucional. Los usuarios del servicio que se retiren de la entidad deben abstenerse de continuar empleándolas y deberá verificar que su cuenta y acceso a los servicios sean cancelados.

El servicio de correo electrónico no debe ser usado 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 sin su autorización.

- Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario como si fuera propia sin la debida autorización.

- Cualquier otro propósito inmoral o ilegal.

Responsabilidades:

El proceso de gestión de seguridad de la información y recursos tecnológicos es responsable de administrar la plataforma tecnológica que soporta el acceso al servicio de correo electrónico corporativo para los funcionarios, contratistas y demás colaboradores que desempeñen labores en el Instituto para la Economía Social.

12.2. 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.

Principios y Aplicabilidad.

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

Los usuarios 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 es responsable tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la red de datos.

Lo usuarios autorizados no podrán descargar software que se encuentre protegido con derechos de autor.

El acceso a redes sociales estará restringido; los usuarios 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, 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 es la responsable de administrar la plataforma tecnológica que soporta el acceso Internet para los funcionarios, contratistas y demás colaboradores que desempeñen labores en la entidad.

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

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

12.3. Política de Control de Acceso.

Objetivo:

Controlar 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, así como evitar la exposición de activos de información y medios de procesamiento de información a daño, perdida, robo o modificación accidental o intencional.

Aplicabilidad:

Esta política aplica a todos los funcionarios y contratistas del Instituto para la Economía Social actuales, que usen su infraestructura.

Detalle de la política:

El Instituto para la Economía Social proporciona a los funcionarios, 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, tabletas, enrutadores, agendas electrónicas, puntos de acceso inalámbrico) que no sean autorizados por el Comité de sistemas y seguridad de la información.

La Subdirección de Diseño y Análisis Estratégico es responsable de suministrar a los usuarios 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.

Es responsabilidad de los usuarios firmar el formato de asignación de credenciales de usuario, a través del cual se compromete a mantener la confidencialidad de las mismas.

Solo personal designado por el proceso de Gestión de la Seguridad de la Información y recursos tecnológicos está autorizado para realizar instalaciones software sobre la infraestructura tecnológica dispuesta a los usuarios del sistema, para lo cual se dispondrá de las credenciales de administrador. Es responsabilidad del equipo de sistemas mantener niveles de seguridad apropiados asociados a la cuenta administrador.

Los usuarios con acceso autorizado a la plataforma tecnológica y áreas de la entidad, son responsables por el manejo que se dé a los activos de información institucional, dependiendo de los roles y responsabilidades establecidas. Es responsabilidad de los

usuarios dar estricto cumplimiento a la política de tratamiento de datos establecida en la entidad.

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.

Las áreas misionales son responsables por el análisis y tratamiento que se dé a la información institucional derivada del uso del sistema de información misional (HEMI). La Subdirección de Diseño y Análisis Estratégico es responsable de la guarda y custodia de la información alojada en el sistema de información misional.

La conexión remota a los servicios informáticos de la entidad, debe ser hecha a través de una conexión VPN (Red Privada Virtual) segura suministrada por la entidad, previa solicitud formal del jefe directo y revisión y autorización del Comité de Sistemas y Seguridad de la Información. El proceso de gestión de la seguridad de la información y recursos tecnológicos podrá realizar monitoreo a las conexiones externas.

Es responsabilidad del Área de Talento Humano informar oportunamente al proceso de gestión de la seguridad y recursos tecnológicos, las novedades relacionadas con los usuarios de la plataforma tecnológica de la entidad, a fin de ejercer un efectivo control sobre los privilegios de acceso.

Es responsabilidad del equipo de sistemas, en desarrollo de la administración de los activos de información (equipos, sistema de información), a intervalos regulares, realizar monitoreo seguimiento y depuración de los privilegios de acceso asignados a los usuarios autorizados.

12.4. Política 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.

Aplicabilidad.

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

Detalle de la política.

El personal del Instituto para La Economía Social 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.

Es responsabilidad de los usuarios 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 puesto de trabajo.

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

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

12.5. Política de Respaldo y Restauración.

Objetivo:

Proporcionar medios de respaldo adecuados para asegurar que todo software e información esencial se pueda recuperar después de una falla.

Aplicabilidad.

Esta política será aplicada por los administradores de tecnología, encargados de sistemas de información 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 como cinta, CD, DVD, discos magnéticos o discos flash entre otros.

El administrador del servidor, de los sistemas de información o los equipos de comunicación es el responsable de definir la frecuencia de respaldo y requerimientos de seguridad de la información en compañía del dueño de la información, y el administrador del sistema de respaldo es el responsable de realizar las pruebas de respaldos periódicas.

Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso tanto físico como lógico.

Las copias de respaldo se guardaran 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 y por requerimientos legales.

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

12.6. Políticas Específicas de Usuario.

Objetivo.

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

Aplicabilidad.

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

Detalle de la Política.

El Instituto para la Economía Social dispone de un espacio de almacenamiento de la información en un servidor de archivos con los permisos necesarios para que cada usuario guarde la información importante y sobre ella se garantizará la disponibilidad en caso de un daño en el equipo asignado al usuario, 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, 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 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 que requieran hacer uso de dispositivos tecnológicos que no hacen parte del inventario de la entidad, deberán ser autorizados por el subdirector o jefe de oficina.

Los programas instalados en los equipos de cómputo de la entidad, son de propiedad del Instituto para la Economía Social, 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 y demás entes rectores de seguridad de la información.

El Instituto para la Economía Social 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 del Instituto para la Economía Social son responsabilidad de los funcionarios.

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

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

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, fotocopiadores, 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 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.

12.7. Políticas Específicas de Personal de Tecnología.

Objetivo.

Definir lineamientos y directrices para asegurar una adecuada protección de los activos de información institucional, por parte de los administradores 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 este 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.

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.

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

Se deben registrar los accesos autorizados al Datacenter. El personal del área de Sistemas debe velar por que se cumpla con el registro en la bitácora de acceso al Datacenter.

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.

12.8. 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 perdida 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.

Principios y 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, sistemas de información, sistemas 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 cobijen a la entidad.

Un sistema de información es cualquier equipo de cómputo o telecomunicaciones, sistema o subsistema 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, 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 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. El 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 los procedimientos internos aprobados para registrar y realizar seguimiento a los incidentes y trabajar con otros funcionarios u organizaciones para tomar las acciones apropiadas como investigar, escalar, remediar, referenciar el incidente a otras organizaciones como lo establecen los procedimientos 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 aceptan formalmente las políticas de seguridad institucionales.

Responsabilidades.

El oficial de seguridad de la información es el responsable por el aislamiento y recuperación de los accesos a sistemas de comunicaciones y cómputo afectados por el incidente. El 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 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 especifico o por iniciativa del Instituto para la Economía Social 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 oficial de seguridad de la información de la entidad debe mantener procedimientos para registro, seguimiento y reporte de incidentes. El 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.

12.9. 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.

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 Oficina Asesora de Control Interno los programas de auditoría del Subsistema de Gestión de Seguridad de la Información.

La Dirección del Instituto para la Economía Social, a través del Comité de 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 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 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 hacia entidades externas, el Instituto para la Economía Social 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.

12.10. Política de Tercerización.

Objetivo.

Mantener la seguridad de la información y los servicios de procesamiento de información a los cuales tienen acceso las partes externas o que son procesados, comunicados o dirigidos por estas.

Aplicabilidad.

La política aplica a toda la entidad. La tercerización 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 deben ser gestionados por medio de controles físicos o lógicos y la implementación de procedimientos legales y administrativos.

- Selección de terceros.

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, otros criterios que resulten de un análisis de riesgos de la selección y los criterios que tenga establecidos la entidad.

- Análisis de riesgos.

Se deben identificar los riesgos de seguridad y los servicios de procesamiento de la información de la entidad en los procesos de negocio que involucren partes externas. 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 de tercerización.

- Consideraciones de seguridad con los clientes.

Para los clientes que tienen acceso a los activos de información de la entidad se deben considerar todos los requisitos de seguridad de información internos para que sean aplicados a los clientes, dentro de estos se encuentran las políticas, convenios, acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual entre otros.

- Acuerdos con terceras 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 intercambiaran 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 de negocio de la entidad.

12.11. Política 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, 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 necesita asegurarse por sistemas criptográficos.

Detalle de la política.

El Comité de Seguridad de la Información de la entidad definirá de acuerdo a la clasificación y análisis de riesgos de la información, que datos deben ser cifrados y su nivel de protección para escoger el tipo de algoritmo criptográfico utilizado.

La Dirección y el Comité de Seguridad de la Información, dará las directrices necesarias para asignar el responsable o responsables de la implementación del sistema criptográfico y el cómo se gestionarán las claves que usa el sistema.

El Comité de Seguridad de la Información del tendrá en cuenta la legislación y marcos normativos vigentes cuando se utilizan sistemas criptográficos sobre la información, en especial la ley 594 de 2000, la ley 527 de 1999 y el decreto 1747 de 2000.

12.12. Política de Comunicaciones 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.

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 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, 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 Seguridad de la Información de la entidad, de acuerdo a las necesidades del negocio definirá las directrices necesarias 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 reglamentan el teletrabajo en Colombia.

12.13. 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 que hacer misional y la adecuada protección de la información de la entidad.

Aplicabilidad.

Estas políticas aplican a todos los usuarios 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 tanto administrativo (GOOBI), como misional (HEMI). El sistema de información misional HEMI, se considera la fuente exclusiva de información necesaria de apoyo al cumplimiento misional.

La Dirección General y la Subdirección de Diseño y Análisis Estratégico tendrán en cuenta los dos sistemas de información como únicas herramientas de apoyo en la toma de decisiones de la Dirección y el seguimiento de los asesores de la SDAE.

Los usuarios 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 Subdirección de Diseño y Análisis Estratégico – Sistemas solo podrá garantizar la protección, el respaldo, la disponibilidad, confidencialidad e integridad de la información derivada del uso de los sistemas de información administrativo (GOOBI) y misional (HEMI).

La información consignada en los sistemas de información del IPES es legalmente del Instituto, no del personal a cargo del registro de información y solo puede emplearse con la finalidad del cumplimiento misional, control administrativo y/o político.

El uso indebido de la información de la entidad, o la negativa a emplear los sistemas de Información (HEMI-GOOBI) serán sujeto de las acciones disciplinarias o legales dispuestas por el Instituto para La Economía Social.

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 de los sistemas de información.

Los usuarios, independiente de la modalidad de vinculación, deben hacer uso de los sistemas de información suministrados por la entidad (HEMI, GOOBI) con el fin de registrar, consolidar, identificar, caracterizar, focalizar, las actuaciones administrativas y los beneficiarios misionales del Instituto para la Economía Social.

Los usuarios solo tendrán acceso a los datos y recursos autorizados por el Instituto para la Economía Social, 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.

La conexión remota empleada para realizar teletrabajo en los sistemas de información del Instituto para la Economía Social 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 Seguridad de la Información, registrada y auditada.

13 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 e instructivo:

- PR-123 GESTION DE INCIDENTES DE SEGURIDAD.
- IN-069 GESTION DE INCIDENTES DE SEGURIDAD

14 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 que 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 procedimiento e instructivo:

- Procedimiento de Manejo de Información Forense.
- Instructivo de Manejo de Información Forense.

15 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.

El Comité de Seguridad de la Información, es responsable de la validación de la existencia del Plan de Contingencia Informático 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, 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.

16 SEGUIMIENTO AL SGSI

El cumplimiento de la normatividad vigente, las disposiciones legales Nacionales y Distritales, y los lineamientos y directrices definidas por el Comité de sistemas y Seguridad de la información, se reglamenta en el presente dominio de la norma técnica internacional, y ofrece a los usuarios de los sistemas y servicios informáticos 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 para hacer seguimiento, monitoreo y control sobre el uso de los sistemas informáticos por parte del talento humano de la entidad, y la aplicación de las políticas de seguridad de la información dispuestas en el presente manual y demás disposiciones legales vigentes y reglamentarias sobre la materia.

Es obligación de todos los funcionarios, servidoras y servidores públicos, Contratistas y Terceros con acceso autorizado los servicios y sistemas informáticos, cumplir con todas las políticas y disposiciones de seguridad digital adoptadas por la entidad.

17 CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO
2		Objetivo	Se realizó revisión integral del documento.
		Alcance	Se cambia el nombre del documento.
		Definiciones	Se ajusta la política general del subsistema de gestión de seguridad de la información.
		Marco Normativo	Se incluye el numeral Marco Normativo
		Política General	Se incluye el numeral de Definiciones.
		Principios que soportan el desarrollo de la política	Se incluyen roles y responsabilidades de seguridad de la información.
		Roles y Responsabilidades	Se eliminan numerales del manual, que son documentos complementarios.