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

IPES

MANUAL DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO

Elaboró: John Jair Garzón – Profesional universitario	Revisó: José del Carmen Montaña Torres - Subdirector de Diseño y Análisis Estratégico	Revisó: José del Carmen Montaña Torres - Subdirector de Diseño y Análisis Estratégico

Bogotá 2014

TABLA DE CONTENIDO

1 INTRODUCCIÓN: 4

2 OBJETIVO: 4

3 ALCANCE: 4

4 RESPONSABLES: 4

5 POLITICA DEL SGSI: 4

6 ALCANCE DEL SGSI: 6

7 METODOLOGIA DE VALORACION DE RIESGOS: 6

7.1 ANÁLISIS DE RIESGOS 6
7.2 EVALUACIÓN DE RIESGOS 7

8 DECLARACIÓN DE APLICABILIDAD: 8

9 PROCEDIMIENTOS OBLIGATORIOS DEL SGSI: 8

9.1 CONTROL DE DOCUMENTOS. 8
9.2 AUDITORÍAS INTERNAS. 8
9.3 ACCIÓN CORRECTIVA. 9
9.4 ACCIÓN PREVENTIVA. 9
9.5 OTROS PROCEDIMIENTOS COMUNES. 9

10 POLÍTICAS COMPLEMENTARIAS DEL SGSI: 10

10.1 POLÍTICA DE USO DE CORREO ELECTRÓNICO. 10
10.2 POLÍTICA DE USO DE INTERNET. 13
10.3 POLÍTICA DE USO DE ANTIVIRUS. 15
10.4 POLÍTICA DE CONTROL DE ACCESO. 17
10.5 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA. 18
10.6 POLÍTICA DE RESPALDO Y RESTAURACIÓN. 18
10.7 POLÍTICAS ESPECÍFICAS DE USUARIO. 19
10.8 POLÍTICAS ESPECÍFICAS DE PERSONAL DE TECNOLOGÍA. 21
10.9 POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. 22
10.10 POLÍTICAS GENERALES DEL NEGOCIO. 24
10.11 POLÍTICA DE TERCERIZACIÓN. 25
10.12 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS 27
10.13 POLÍTICA DE COMUNICACIONES MÓVILES Y TELETRABAJO. 27
10.14 POLITICA DE EMPLEO DEL SISTEMAS DE INFORMACIÓN 28

11 PROCEDIMIENTO DE INCIDENTES DE SEGURIDAD: 29

12 PROCEDIMIENTO DE LEVANTAMIENTO DE INFORMACIÓN FORENSE: 30

13 RESULTADOS ANÁLISIS DE RIESGOS: 30

14 PLAN DE IMPLEMENTACIÓN DEL SGSI: 32

14.1 COMPONENTES DEL PLAN DE IMPLEMENTACIÓN 32
14.2 DESARROLLO DEL PLAN DE IMPLEMENTACIÓN DEL SGSI 34
14.3 ACCIONES PARTICULARES A SEGUIR 35

15 CONTROLES SELECCIONADOS DEL SGSI: 42

16 CONTROL DE CAMBIOS AL DOCUMENTO: 58

1 INTRODUCCIÓN:

De acuerdo a las políticas del Gobierno Distrital y en cumplimiento a la resolución 305 de 2008 se requiere establecer los mecanismos para asegurar la confidencialidad, integridad, disponibilidad y confiabilidad de la información que se maneja al interior de la entidad y la que se proporciona a sus clientes.

2 OBJETIVO:

Definir el conjunto de políticas, procedimientos, metodologías y controles enfocados en garantizar un desempeño institucional articulado y armónico que busque de manera constatable la satisfacción del subsistema de gestión de seguridad de la información.

3 ALCANCE:

Todos los elementos establecidos en el presente manual, aplican al personal, contratistas y terceras partes del INSTITUTO PARA LA ECONOMIA SOCIAL y hacen parte de su Sistema Integrado de Gestión.

4 RESPONSABLES:

Es responsabilidad del Comité Integrado de Gestión del IPES y el Comité de Seguridad de la Información o Comité de Sistemas, que el manual del Subsistema de Gestión de Seguridad de la Información se mantenga controlado y correlacionado con el Sistema Integrado de Gestión.

Niveles de autoridad y responsabilidad de documentos:

Control de la Documentación	Responsable
Elaborar	Profesional responsable del proceso
Revisar	Subdirector y/o Jefe de Oficina responsable del proceso.
Aprobar	Subdirector y/o Jefe de Oficina responsable del proceso.
Divulgar	Subdirector y/o Jefe de Oficina responsable del proceso.
Anular	Comité de archivo

5 POLITICA DEL SGSI:

Debido a que la información es uno de los activos más importantes de la organización, La Dirección del Instituto Para la Economía Social IPES por medio del Subsistema de

Gestión de Seguridad de la Información del Sistema Integrado de Gestión, tiene como propósito de esta política garantizar la seguridad de la información en aspectos tales como la confidencialidad, integridad y disponibilidad de la información, contribuyendo con el diseño y desarrollo de alternativas productivas, acordes a las políticas públicas del sector de desarrollo económico de Bogotá y en concordancia con los estándares establecidos por la Comisión Distrital de Sistemas.

Cumplir con los requerimientos legales, reglamentarios, contractuales y establecidos por la normatividad nacional y distrital, e internos de la organización en cuanto a seguridad de la información.

Garantizar la confiabilidad de la información que le es provista a los diferentes tipos de usuarios del IPES, mediante el desarrollo e implantación de controles a los proyectos que hagan uso de tecnologías de información y comunicaciones.

Establecer los requisitos de seguridad de la información y gestionar los mecanismos para evaluar y tratar los riesgos de acuerdo a la metodología de gestión de riesgos establecida por el Sistema Integrado de Gestión del IPES.

Todos los subdirectores y jefes de oficinas asesoras son responsables directos de la implementación de la Política de Seguridad de la Información, en lo referente a sus áreas de negocio y a su personal.

Es responsabilidad de todo el personal informar rápidamente de los incidentes y brechas de seguridad de la información, reales o bajo sospecha, los que deben ser tratados oportunamente. La organización debe asegurar la formación, capacitación y concienciación a todo el personal del IPES en seguridad de la información.

Producir, mantener y probar los planes que garanticen la continuidad de las operaciones ante una situación crítica que pueda amenazar parcial o totalmente la prestación de servicios de la organización.

Objetivos del SGSI.

- Garantizar la prestación de servicios de información y tecnología con calidad, eficiencia y efectividad.
- Mejorar la capacidad organizacional para mantener la continuidad en la prestación del servicio al ciudadano.
- Mejorar las capacidades internas para la atención de incidentes de seguridad de la información.
- Fortalecer las competencias del talento humano para la protección de la información.

6 ALCANCE DEL SGSI:

El subsistema de gestión de seguridad de la información adoptado para el Instituto para la Economía Social -IPES- hace parte del Sistema Integrado de Gestión.

El alcance del subsistema de gestión de seguridad de la información comprende los procesos misionales de la entidad, complementado con los procesos de apoyo de Gestión Documental y Gestión de Procesos Tecnológicos que son procesos transversales a la entidad.

7 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 estimarel riesgo) y la evaluación de riesgos.

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

7.1 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 componentes de tecnología) 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 del impacto

El cálculo del impacto se realiza de forma cuantitativa teniendo en cuenta las consecuencias de la pérdida de la confidencialidad, integridad o disponibilidad de los activos.

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.

7.2 Evaluación de Riesgos

Priorización de riesgos y cálculo del riesgo residual

Una vez estimados los niveles de riesgo, estos se deben ordenar y priorizar para la realización del respectivo tratamiento del riesgo con el fin de encontrar un orden en ese tratamiento, es decir empezar por los riesgos más extremos. Para cada riesgo verificamos si hay un control existente que lo pueda mitigar o si es necesario complementar ese control o aplicar 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.

8 DECLARACIÓN DE APLICABILIDAD:

La declaración de aplicabilidad (también denominada SOA por sus siglas en inglés) es un documento clave e importante para el Subsistema de Gestión de Seguridad de la información del IPES. En este documento se detallan los 133 controles sugeridos por la norma ISO 27001:2005 y se establecen cuáles son aplicables y cuáles no. El documento detallado de declaración de aplicabilidad del IPES se encuentra en el documento "**SOA_IPES**".

9 PROCEDIMIENTOS OBLIGATORIOS DEL SGSI:

Los sistemas de gestión en general tienen muchos elementos en común, por lo que si se ha implementado un sistema o varios sistemas de gestión, estos elementos comunes pueden ser utilizados para el nuevo sistema.

Los sistemas de gestión en general (calidad, ambiental, seguridad de la información, etc.), se han desarrollado basados en el modelo PHVA (planear, hacer, verificar y actuar) y el modelo de operación por procesos, de ahí que se realizan tablas de equivalencia entre los diferentes sistemas de gestión, ejercicio que lo sugiere la Norma Técnica Distrital del Sistema Integrado de GestiónNTD-SIG 001:2011.

De acuerdo a lo anterior se tomarán algunos procedimientos del documento "**DE-014 MANUAL DE OPERACIONES capítulo III MANUAL DE CALIDAD**".

9.1 Control de Documentos.

Los documentos exigidos por el SGSI se deben proteger y controlar. Para el efectivo control de la documentación se han definido los siguientes instrumentos:

- Procedimiento Control de documentos internos Código PR-005
- Norma básica para la elaboración de documentos Código IN-001

Control de Registros.

Para el efectivo control de los registros y con el propósito de proporcionar evidencia de la conformidad con los requisitos así con la operación eficaz del sistema, se ha definido el siguiente procedimiento e instrumentos complementarios:

- Procedimiento Control de los Registros Código PR-006.
- IN-005 Manejo de los archivos IPES
- IN-006 radicación

9.2 Auditorías Internas.

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

9.3 Acción Correctiva.

La entidad debe emprender acciones para eliminar la causa de no conformidades asociadas con los requisitos del SGSI, con el fin de prevenir que ocurran nuevamente. Se ha definido el siguiente procedimiento:

- Procedimiento de acciones correctivas PR-003

9.4 Acción Preventiva.

La entidad debe determinar acciones para eliminar la causa de no conformidades potenciales con los requisitos del SGSI y evitar que ocurran. Se ha definido el siguiente procedimiento:

- Procedimiento de acciones preventivas PR-002

9.5 Otros Procedimientos Comunes.

- **Gestión del Talento Humano** PO-009, Procedimiento Nómina PR-015, con los instructivos: IN-025 Archivo y actualización de hojas de vida, IN-026 Expedición de certificaciones, IN-036 Administración plan de capacitación, IN-039 Evaluación de desempeño, IN-041 Administración de la carrera administrativa.
- **Gestión de Recursos Físicos** PO-010, con los instructivos: IN-003 Formulación del plan de compras y contratación, IN-008 Baja de bienes devolutivos, IN-009 Ingreso de bienes a recursos físicos, IN-010 Manejo de servicios públicos, IN-011 Salida de bienes, IN-012 Traslado de bienes de bodega a servicio y entre funcionarios, IN-013 Traslado temporal de bienes entre entidades, IN-014 Baja elementos de consumo y consumo controlado, IN-015 Levantamiento físico de inventarios, IN-016 Reintegro de bienes devolutivos en servicio, IN-017 Solicitud de pedido de elementos de consumo, IN-018 Traslado temporal de bienes a recursos físicos, IN-033 Ingreso de personal, IN-034 Vigilancia, mantenimiento y servicios generales.
- **Gestión de Recursos Tecnológicos**PO-013, Procedimientos: PR-030 Administración de usuarios, PR-031 Administración del portal, PR-033 Backup generación y recuperación, PR-034 Solicitud de mantenimiento de equipos de cómputo, PR-035 Préstamo de software, PR-036 Seguridad en los servicios de red, con los instructivos: IN-002 Instructivo línea 195, IN- 043 Backup de equipos clientes IPES, IN- 044 Configuración Microsoft office Outlook a dominio IPES, IN- 045 Configuración en red impresora HP 2420, IN- 046 Configuración archivos PST correo en Outlook 2003, IN- 047 Configuración archivos PST correo en Outlook 2007, IN- 048 Instalación del agente MCAFEE.
- **Revisión por la Dirección**: La mejora continua es el objetivo principal del Sistema de Gestión de la Calidad del Instituto para la Economía Social -IPES-, para el efecto la alta dirección a determinado llevar a cabo revisiones periódicas (1 vez cada año) que le permiten evaluar el funcionamiento, la conveniencia, adecuación, eficacia, eficiencia y efectividad del sistema y su sostenibilidad. De acuerdo a lo anterior el Subsistema de Gestión de Seguridad

de la Información hará las revisiones por la dirección de acuerdo al cronograma estipulado por el Sistema Integrado de Gestión del IPES.

10 POLÍTICAS COMPLEMENTARIAS DEL SGSI:

10.1 Política de uso de correo electrónico.

Objetivo.

Definir las pautas generales para asegurar una adecuada protección de la información del INSTITUTO PARA LA ECONOMIA SOCIAL cuando se usa el servicio de correo electrónico por parte de los usuarios autorizados.

Principios y Aplicabilidad.

Esta es una política del INSTITUTO PARA LA ECONOMIA SOCIAL que 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 y de evitar prácticas o usos que puedan comprometer la seguridad de la información del INSTITUTO PARA LA ECONOMIA SOCIAL.

El servicio debe ser empleado para servir a una finalidad operativa y administrativa en relación con el INSTITUTO PARA LA ECONOMIA SOCIAL. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad del INSTITUTO PARA LA ECONOMIA SOCIAL y pueden ser escaneadas por el administrador del servicio y revisadas por las instancias de vigilancia y control distritales y nacionales.

Detalle de la Política.

Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en el INSTITUTO PARA LA ECONOMIA SOCIAL y no debe utilizarse para ningún otro fin.

El acceso al servicio podrá ser asignado a las personas que tengan algún tipo de vinculación con el INSTITUTO PARA LA ECONOMIA SOCIAL, ya sea como funcionario, contratista o colaborador y para las cuales un funcionario de nivel directivo lo solicite formal y expresamente.

El servicio debe utilizarse única y exclusivamente para las tareas propias de la función desarrollada en el INSTITUTO PARA LA ECONOMIA SOCIAL y no debe utilizarse para ningún otro fin.

La clave de acceso al servicio es la mejor defensa contra el uso no autorizado al servicio de correo del INSTITUTO PARA LA ECONOMIA SOCIAL, por lo tanto se

requiere que se mantenga con la mayor reserva posible, no debe suministrarse a otras personas o exhibirse en público.

El único servicio de correo electrónico autorizado en la entidad es el asignado directamente por el Área de Sistemas, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de malware. Además este servicio tiene respaldo de diferentes procesos de copia de respaldo aplicados de manera periódica y segura.

El INSTITUTO PARA LA ECONOMIA SOCIAL puede supervisar cualquier cuenta de correo para certificar que se está usando para los propósitos legítimos. El incumplimiento de la presente política puede conducir a acciones disciplinarias tales como terminación de la relación laboral o acciones de índole legal.

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 el INSTITUTO PARA LA ECONOMIA SOCIAL.

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.

La encriptación del correo electrónico no es necesaria en la mayoría de situaciones, pero los mensajes confidenciales deben tener alguna forma de codificación. En caso de dudas contacte al Área de Sistemas.

Los usuarios deben seleccionar correctamente los destinatarios. En la mayoría de situaciones se deben enviar correos electrónicos a correos corporativos de otras entidades.

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

El tamaño del buzón de correo electrónico se asignará de acuerdo con el rol que desempeña el usuario en el INSTITUTO PARA LA ECONOMIA SOCIAL, la capacidad específica será definida y administrada por el Área de Sistemas.

Si una cuenta de correo es capturada por hackers o se reciben excesiva cantidad de correo no deseado (SPAM), una nueva cuenta será generada y la anterior será borrada.

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 INSTITUTO PARA LA ECONOMIA SOCIAL.

Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de acceso a la red y al servicio de correo corporativo se retire del INSTITUTO PARA LA ECONOMIA SOCIAL, deberá 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, tales como contenidos ofensivos, obscenos, pornográficos, chistes, terroristas, o cualquier contenido que represente riesgo de malware.
- Envío o intercambio de mensajes que promuevan la discriminación sobre la base de raza, género, nacionalidad de origen, edad, estado marital, orientación sexual, religión o discapacidad.
- Envío de mensajes que contengan amenazas o mensajes violentos.
- Creación, almacenamiento o intercambio de mensajes que violen las leyes de material protegido por la ley de derechos de autor.
- Distribuir información del INSTITUTO PARA LA ECONOMIA SOCIAL clasificada como no pública, 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 área de Talento Humano es la responsable de solicitar la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de correo electrónico corporativo al Área de Sistemas.

Todos los funcionarios, contratistas y demás colaboradores, en el desarrollo de sus tareas habituales u ocasionales, que utilicen cualquier servicio de tecnología de

información y comunicaciones (TIC) que provea el INSTITUTO PARA LA ECONOMIA SOCIAL son responsables del cumplimiento y seguimiento de esta política.

El Área de Sistemas es la 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 ECONOMIA SOCIAL.

El Área de Sistemas se reserva el derecho de escanear el servicio de correo electrónico corporativo.

El Área de Sistemas se reserva el derecho de filtrar los contenidos que se trasmitan en la red del INSTITUTO PARA LA ECONOMIA SOCIAL y en uso del servicio del correo electrónico corporativo.

10.2 Política de Uso de Internet.

Objetivo.

Definir las pautas generales para asegurar una adecuada protección de la información del INSTITUTO PARA LA ECONOMIA SOCIAL en el uso del servicio de Internet por parte de los usuarios autorizados.

Principios y Aplicabilidad.

Esta es una política del INSTITUTO PARA LA ECONOMIA SOCIAL que 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 la información del INSTITUTO PARA LA ECONOMIA SOCIAL.

El servicio debe ser empleado para servir a una finalidad operativa y administrativa en relación con el INSTITUTO PARA LA ECONOMIA 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 el INSTITUTO PARA LA ECONOMIA SOCIAL y no debe utilizarse para ningún otro fin.

El acceso al servicio podrá ser asignado a las personas que tengan algún tipo de vinculación con el INSTITUTO PARA LA ECONOMIA SOCIAL, ya sea como funcionario, contratista o colaborador y para las cuales un funcionario de nivel directivo lo solicite formal y expresamente.

El navegador autorizado para el uso del servicio de Internet en el INSTITUTO PARA LA ECONOMIA SOCIALes el designado por el Área de Sistemas, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

Los servicios a los que un determinado usuario pueda acceder desde Internet dependerán del rol que desempeña el usuario en el INSTITUTO PARA LA ECONOMIA SOCIALy para los cuales este formal y expresamente autorizado.

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 INSTITUTO PARA LA ECONOMIA SOCIAL.

Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de acceso a la red y al servicio de Internet, se retire del INSTITUTO PARA LA ECONOMIA SOCIAL, deberá abstenerse de continuar empleándolas y deberá verificar que su cuenta y acceso a los servicios sean cancelados.

Todo usuario es responsable tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la red del INSTITUTO PARA LA ECONOMIA SOCIALo descargue desde Internet.

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 por INSTITUTO PARA LA ECONOMIA SOCIAL.
- Cualquier otro propósito considerado inmoral o ilegal.

Responsabilidades.

El área de Talento Humano es la responsable de solicitar la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de Internet al Área de Sistemas.

Todos los funcionarios, contratistas y demás colaboradores 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 ECONOMIA SOCIAL son responsables del cumplimiento y seguimiento de esta política.

El Área de Sistemas es la responsable de administrar la plataforma tecnológica que soporta el acceso a la red/cuentas de usuario o al servicio de Internet para los

funcionarios, contratistas y demás colaboradores que desempeñen labores en el INSTITUTO PARA LA ECONOMIA SOCIAL.

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

El Área de Sistemas se reserva el derecho de filtrar los contenidos que se reciban desde Interneto se envíen desde la red del INSTITUTO PARA LA ECONOMIA SOCIAL.

10.3 Política de Uso de Antivirus.

Objetivo.

Definir las pautas generales para asegurar una adecuada protección de la información del INSTITUTO PARA LA ECONOMIA SOCIAL contra malware.

Principios y Aplicabilidad.

Esta es una política del INSTITUTO PARA LA ECONOMIA SOCIAL que aplica a toda la entidad y a todos los usuarios autorizados para utilizar este servicio.

Los usuarios de los servicios TIC del INSTITUTO PARA LA ECONOMIA SOCIAL son responsables de la utilización de programas antivirus para analizar, verificar y si es posible eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos o removibles o los archivos o el correo electrónico que esté autorizado a emplear.

EL INSTITUTO PARA LA ECONOMIA SOCIAL contará permanentemente con los programas antivirus de protección a nivel de red y de estaciones de trabajo, contra virus o código malicioso, el servicio será administrado por el Área de Sistemas.

Los programas antivirus deben ser instalados por el Área de Sistemas en los equipos centralizados de procesamiento y en las estaciones de trabajo de modo residente para que estén activos durante su uso.

Se deben actualizar periódicamente las versiones de los programas antivirus y dicha situación debe estar reflejada en los contratos con los proveedores.

Detalle de la Política.

Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en el INSTITUTO PARA LA ECONOMIA SOCIAL y no debe utilizarse para ningún otro fin.

Verificar frecuentemente con las herramientas (software) antivirus instaladas en el computador o dispositivos la no presencia de virus o código malicioso en los

dispositivos de almacenamiento fijos o removibleso archivos en los computadores o dispositivos informáticos que esté autorizado a emplear.

Ejecutar el escaneo de virus con las herramientas antivirus provistos cada vez que detecte que algún equipo o dispositivo informático funcionando de manera irregular o se sospeche de la presencia de virus en equipos, dispositivos, archivos o correos electrónicos.

El servicio de antivirus corporativo no requiere de solicitud o autorización para su uso.

Todo usuario es responsable por la destrucción de archivos o mensajes que les hayan sido enviados por cualquier medio, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta soporte@ipes.gov.co con la frase “correo sospechoso” en el asunto.

El único servicio de antivirus autorizado en la entidad es el asignado directamente por el Área de Sistemas, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso. Además este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura. Excepcionalmente se podrá realizar la ejecución de otro programa antivirus, únicamente por personal autorizado por el Área de Sistemas, a efectos de reforzar el control de presencia y/o programación de virus y/o código malicioso.

Este servicio no debe ser usado para:

- Abrir o descargar archivos o documentos de remitente desconocido, no confiable o sospechoso. En lo posible deberán ser borrados de las carpetas donde se encuentren y eliminarlos de la papelera del computador.
- Intercambio de archivos que hayan sido identificados como infectados por virus o código malicioso o sean sospechosos de estar infectados.
- Desactivar o eliminar los programas antivirus o de detección de código malicioso en los equipos o sistemas en que estén instalados.
- Instalar o emplear programas no autorizados.
- Instalar, conectar o emplear dispositivos de almacenamiento fijos o removibles o archivos en los computadores o dispositivos informáticos no autorizados.

Responsabilidades.

Todos los funcionarios, contratistas y demás colaboradores que, en el desarrollo de sus tareas habituales u ocasionales, utilicen cualquier servicio de tecnología de la

información y comunicaciones (TIC) o manipulen equipos pertenecientes a la red que provea el INSTITUTO PARA LA ECONOMIA SOCIALson responsables del cumplimiento y seguimiento de esta política.

El Área de Sistemas es la responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los computadores o equipos informáticos de la red del INSTITUTO PARA LA ECONOMIA SOCIALque son empleados por funcionarios, contratistas y demás colaboradores que desempeñen labores en la entidad.

El Área de Sistemas se reserva el derecho de escanear las comunicaciones o la información que se generen, comuniquen, tramitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.

El Área de Sistemas se reserva el derecho de filtrar los contenidos que se trasmitan en la red del INSTITUTO PARA LA ECONOMIA SOCIALpara evitar amenazas de virus. Todos los correos electrónicos serán escaneados para verificar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.

10.4 Política de Control de Acceso.

Objetivo.

Definir las pautas generales para asegurar un acceso controlado a la información, las aplicaciones y las redes del INSTITUTO PARA LA ECONOMIA SOCIAL, así como el uso de medios de computación móvil y teletrabajo.

Aplicabilidad.

Esta política aplica a todos los funcionarios y contratistas del INSTITUTO PARA LA ECONOMIA SOCIAL actuales o por ingresar, que usen su infraestructura.

Detalle de la política.

El INSTITUTO PARA LA ECONOMIA SOCIAL proporciona a los empleados todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos (móviles o fijos tales como portátiles, celulares, tabletas, teléfonos inteligentes, enrutadores, agendas electrónicas, puntos de acceso inalámbrico) que no sean autorizados por el Comité de Seguridad de la Información y el Área de Sistemas.

El INSTITUTO PARA LA ECONOMIA SOCIAL suministra a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.

Solo personal designado por el Área de Sistemas está autorizado para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones del INSTITUTO PARA LA ECONOMIA SOCIAL.

Todo trabajo que utilice los servidores del INSTITUTO PARA LA ECONOMIA SOCIAL con información de los clientes o la organización se debe realizar en sus instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación delINSTITUTO PARA LA ECONOMIA SOCIAL.

La conexión remota a la red de área local del INSTITUTO PARA LA ECONOMIA 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.

10.5 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 del INSTITUTO PARA LA ECONOMIA SOCIAL actuales o por ingresar, que usen su infraestructura.

Detalle de la política.

El personal del INSTITUTO PARA LA ECONOMIA SOCIALdebe 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.

El personal del INSTITUTO PARA LA ECONOMIA SOCIAL debe bloquear la pantalla de su computador 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.

10.6 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, el sistema 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.

10.7 Políticas Específicas de Usuario.

Objetivo.

Definir las pautas generales para asegurar una adecuada protección de la información del INSTITUTO PARA LA ECONOMIA SOCIAL por parte de los usuarios de la entidad.

Aplicabilidad.

Estas políticas aplican a todos los funcionarios delINSTITUTO PARA LA ECONOMIA SOCIAL actuales o por ingresar.

Detalle de la Política.

El INSTITUTO PARA LA ECONOMIA SOCIAL suministra una cuota 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 INSTITUTO PARA LA ECONOMIA SOCIAL únicamente a través del personal del Área de Sistemas, instalara copias de los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades necesarias para suplir sus necesidades. 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 ECONOMIA 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 tanto está prohibido su uso si este no ha sido autorizado individualmente.

Los programas instalados en los equipos son de propiedad del INSTITUTO PARA LA ECONOMIA SOCIAL, la copia no autorizada de programas legales o de su documentación, implica una violación a la política general del INSTITUTO PARA LA ECONOMIA SOCIAL. 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 ECONOMIA SOCIAL.

El INSTITUTO PARA LA ECONOMIA 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 ECONOMIA 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 por el INSTITUTO PARA LA ECONOMIA SOCIAL para estos propósitos.

Los usuarios solo tendrán acceso a los datos y recursos autorizados por el INSTITUTO PARA LA ECONOMIA 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 organización.

Los equipos que se encuentren fuera de las instalaciones del INSTITUTO PARA LA ECONOMIA SOCIAL no deben dejarse en sitios públicos sin una adecuada vigilancia.

Los equipos como portátiles del INSTITUTO PARA LA ECONOMIA SOCIAL deben ser tratados y llevados como equipaje de mano. En caso de llevar varios equipos, debe contratarse un servicio de transporte adecuado.

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 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 área local del INSTITUTO PARA LA ECONOMIA 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.

10.8 Políticas Específicas de Personal de Tecnología.

Objetivo.

Definir las pautas generales para asegurar una adecuada protección de la información del INSTITUTO PARA LA ECONOMIA SOCIAL por parte de los administradores de TI de la entidad.

Aplicabilidad.

Estas políticas aplican al personal del Área de Sistemas del INSTITUTO PARA LA ECONOMIA SOCIAL, 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 PCs y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor.

No se pueden hacer copias de programas o su documentación sin el consentimiento por escrito del INSTITUTO PARA LA ECONOMIA SOCIAL y del proveedor.

El personal del área de Sistemas debe velar por que se cumpla con el registro en la bitácora de acceso al Datacenter, de las personas que ingresen y que hayan sido autorizadas previamente por el Área de Sistemas.

Por defecto, en los servidores, todos los protocolos y servicios deben ser bloqueados, no se debe permitir ninguno a menos que sea solicitado 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.

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

Objetivo.

Proteger la integridad, disponibilidad y confidencialidad de la 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 (“incidente”) es cualquier evento que daña o representa una amenaza seria para toda o una parte de la infraestructura de información y tecnología del INSTITUTO PARA LA ECONOMIA SOCIAL (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 del INSTITUTO PARA LA ECONOMIA SOCIAL. 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 recursos de información y tecnología del INSTITUTO PARA LA ECONOMIA SOCIAL, 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 del INSTITUTO PARA LA ECONOMIA SOCIALy 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.

Cualquier funcionario del INSTITUTO PARA LA ECONOMIA SOCIAL, contratista o entidades externas pueden reportar eventos relacionados con la seguridad de la información al [oficial o encargado de seguridad de la información] del INSTITUTO PARA LA ECONOMIA SOCIAL. El [oficial o encargado 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 o encargado de la 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 del INSTITUTO PARA LA ECONOMIA SOCIAL.

Responsabilidades.

El [oficial o encargado 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 o encargado 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 o encargado 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 sistema integrado de gestión. Los reportes de incidentes deben ser remitidos por el [oficial o encargado de seguridad de la información] al [Comité de Sistemas de la entidad o el que designe la entidad], el [oficial o encargado 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 ECONOMIA 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 el INSTITUTO PARA LA ECONOMIA SOCIAL.

Cuando sea factible, el INSTITUTO PARA LA ECONOMIA SOCIAL 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 o encargado de seguridad de la información] del INSTITUTO PARA LA ECONOMIA SOCIAL debe mantener procedimientos para registro, seguimiento y reporte de incidentes. El [oficial o encargado 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.

10.10 Políticas Generales del Negocio.

Objetivo.

Definir las pautas de propósito general del negocio para asegurar una adecuada protección de la información del INSTITUTO PARA LA ECONOMIA 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 ECONOMIA 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 ECONOMIA 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 ECONOMIA 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 ECONOMIA 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 ECONOMIA SOCIAL hacia entidades externas, El INSTITUTO PARA LA ECONOMIA 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 ECONOMIA SOCIAL, esta revisión debe quedar documentada.

10.11 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 entidaden 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.

10.12 Política de Controles Criptográficos.

Objetivo.

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

Aplicabilidad.

Esta política aplicapara 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 suclasificación necesita asegurarse por sistemas criptográficos.

Detalle de la política.

El Comité de Seguridad de la Información del INSTITUTO PARA LA ECONOMIA SOCIAL 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 del INSTITUTO PARA LA ECONOMIA SOCIAL dará las directrices necesarias para asignar el responsable o responsables de laimplementacióndel sistema criptográfico y el cómo se gestionarán las claves que usa el sistema.

El Comité de Seguridad de la Información del INSTITUTO PARA LA ECONOMIA SOCIAL 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.

10.13 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 aplicapara 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 Seguridad de la Información del INSTITUTO PARA LA ECONOMIA 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 las redes del INSTITUTO PARA LA ECONOMIA SOCIAL.

La Dirección y El Comité de Seguridad de la Información del INSTITUTO PARA LA ECONOMIA SOCIAL 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.

10.14. Políticas de empleo de Sistemas de Información

Objetivo.

Delimitar 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 del INSTITUTO PARA LA ECONOMIA SOCIAL.

Aplicabilidad.

Estas políticas aplican a todos los funcionarios del INSTITUTO PARA LA ECONOMIA SOCIAL actuales o por ingresar.

Detalle de la Política.

El INSTITUTO PARA LA ECONOMIA SOCIAL suministra los sistemas de información tanto administrativo (SIAFI), como misional (HEMI) como exclusivas herramientas 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 alta dirección y el seguimiento de los asesores de la SDAE.

Los funcionarios y colaboradores 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.

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 se puede emplearse con la finalidad del cumplimiento misional, control administrativo y/o político.

El uso indebido de la información del Instituto o la negativa a emplear los sistemas de Información (HEMI-SIAFI) serán sujeto de las acciones disciplinarias o legales dispuestas por el INSTITUTO PARA LA ECONOMIA SOCIAL.

El INSTITUTO PARA LA ECONOMIA 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.

El personal del Instituto, independiente de la modalidad de contratación, debe hacer uso de los sistemas de información que le ofrece la entidad (HEMI, SIAFI) con el fin de registrar, consolidar, identificar, caracterizar, focalizar, las actuaciones administrativas y los beneficiarios misionales del INSTITUTO PARA LA ECONOMIA SOCIAL.

Los usuarios solo tendrán acceso a los datos y recursos autorizados por el INSTITUTO PARA LA ECONOMIA 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 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 empleada para realizar teletrabajo en los sistemas de información del INSTITUTO PARA LA ECONOMIA 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.

11 PROCEDIMIENTO DE INCIDENTES DE SEGURIDAD:

El procedimiento establece los métodos estándar para identificar, realizar seguimiento y responder a los incidentes de seguridad de la información del INSTITUTO PARA LA ECONOMIA SOCIAL. Se ha definido el siguiente procedimiento e instructivo:

- Procedimiento de Manejo de Incidentes de Seguridad.
- Instructivo de Manejo de Incidentes de Seguridad.

12 PROCEDIMIENTO DE LEVANTAMIENTO DE INFORMACIÓN FORENSE:

El procedimiento permite 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.

13 RESULTADOS ANÁLISIS DE RIESGOS:

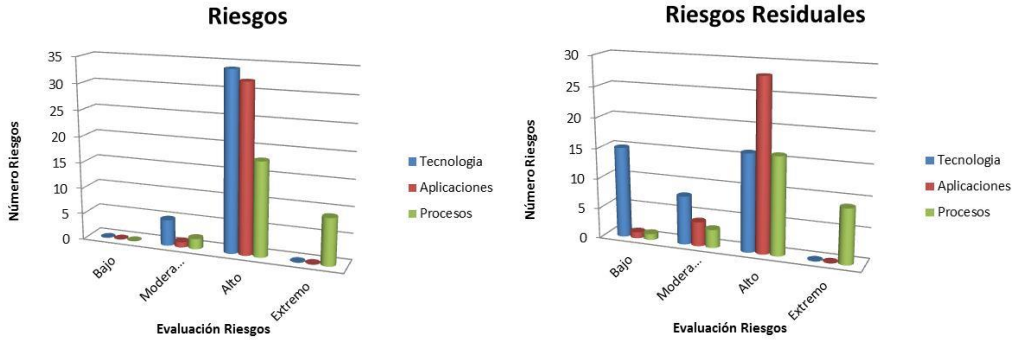
El análisis de riesgos de seguridad de la información se hizo con base en sus activos de información, que de acuerdo a la definición de la norma NTC-ISO/IEC 27001 son “cualquier cosa que tenga valor para la organización”, como ejemplo de activos tenemos los procesos de la organización (estratégicos, misionales, apoyo), información, personas, equipos, sistemas de información, entre otros. Los activos pueden clasificarse como primarios y de soporte; dentro de los activos primarios tenemos como ejemplo los procesos de la organización y la información, dentro de los activos de soporte tenemos las personas, hardware y software entre otros.

En la gráfica 1 se puede apreciar el porcentaje de distribución de los riesgos encontrados en los activos analizados,este riesgo corresponde al obtenido de acuerdo al impacto que se produce y la probabilidad de que ocurra que una amenaza aproveche la debilidad o vulnerabilidad de un activo de información. En la misma gráfica 1 se puede apreciar el porcentaje de distribución de los riesgos residuales, que son los que resultan de hacer un recalculo del riesgo luego de que se aplique algún control que permita disminuir o mitigar el riesgo inicial calculado.

Se debe resaltar el hecho de que muchos de los riesgos identificados como extremos no cambian su calificación debido a que algunos de los controles existentes en el IPES son inefectivos o no se aplican correctamente lo que implica que los riesgos persisten pese a los controles.

Gráfica 1. Riesgos y Riesgos Residuales IPES.

En la gráfica 2 se puede apreciar la distribución del número de riesgos y riesgos residuales versus la estimación del riesgo, clasificados de acuerdo al tipo de activo. La diferencia entre las dos distribuciones se debe a los controles existentes en la entidad. Se debe considerar que el proceso de tecnología por ser un proceso de apoyo y transversal de la entidad, algunos de sus riesgos pueden llegar a afectar a otros activos como lo son los procesos misionales y la información en general.



Gráfica 2. Riesgos y Riesgos Residuales por Tipos de Activos IPES.

El análisis de riesgos no es una tarea de una sola vez, sino una tarea continua en la que deben participar el recurso humano como el eslabón más débil en un sistema de gestión de seguridad de la información. Es por esto que deben realizarse actividades de socialización del sistema y asegurarse que han sido entendidas y están en capacidad de seguir y acatar las políticas y directrices de la organización.

Para la mitigación de los riesgos, debe entenderse que no solo existen la tecnología y los equipos, sino que debe pensarse en controles de tipo administrativo como lo son las políticas, directrices, buenas prácticas y concienciación en seguridad de la información.

14 PLAN DE IMPLEMENTACIÓN DEL SGSI:

Este plan relaciona las acciones recomendadas a corto mediano y largo plazo para lograr la implementación del sistema de gestión de seguridad de la información del INSTITUTO PARA LA ECONOMIA SOCIAL. La implementación del sistema se debe realizar dentro de la coordinación del sistema integrado de gestión que ya existe en la entidad.

14.1 Componentes del plan de implementación

Se describen los puntos en donde se pueden encontrar los componentes para la implementación del SGSI del INSTITUTO PARA LA ECONOMIA SOCIAL.

Estructura Organizacional de seguridad de la información.

Se debe contar con un comité interdisciplinario responsable de la dirección estratégica del SGSI, el comité de sistemas actual puede asumir este rol. Debe existir un [oficial o un encargado de seguridad de la información] encargado de la gestión del sistema, y un conjunto de responsabilidades separadas entre las áreas de tecnología y las áreas usuarias para el apropiado apoyo a la gestión de la seguridad de la información en el INSTITUTO PARA LA ECONOMIA SOCIAL.

Clasificación de información

En el proceso de consultoría se suministró el documento: MODELO DE CLASIFICACIÓN DE INFORMACIÓN, el documento proporciona los diferentes niveles de clasificación de la información, los cuales fueron acordados y socializados en una charla taller con las diferentes áreas del INSTITUTO PARA LA ECONOMIA SOCIAL.

Políticas y procedimientos de la gestión de seguridad

En el proceso de consultoría se suministró el Manual del Subsistema de Gestión de Seguridad de la Información donde se encuentran las políticas del subsistema de gestión de seguridad de la información.

Controles tecnológicos

Como parte del proceso de consultoría se suministró la declaración de aplicabilidad (SOA) del subsistema de gestión de seguridad de la información, el cual como lo específica la norma NTC ISO 27001:2005 contiene:

- Los controles seleccionados
- Los controles implementados actualmente
- Las justificaciones de selección o no de los controles

Gestión del recurso humano

El comité de sistemas o el que el INSTITUTO PARA LA ECONOMIA SOCIAL designe debe definir los roles y responsabilidades recomendados por los diferentes estándares

de gestión de la seguridad de la información para los encargados de seguridad de la información, debe garantizar una socialización y concientización a todo el personal de la entidad en el conocimiento de las amenazas y responsabilidades por salvaguardar la confidencialidad, integridad y disponibilidad de la información.

Monitoreo y revisión de la gestión de seguridad

Debido a que el INSTITUTO PARA LA ECONOMIA SOCIAL ya cuenta con un sistema integrado de gestión que considera los componentes para la supervisión, seguimiento y mejora continua, los resultados de la consultoría se concentraron en sugerir fortalecer el esquema de control de registros de auditoría de los diferentes sistemas de información, así como la gestión y monitoreo centralizado de los elementos de tecnología de la información del INSTITUTO PARA LA ECONOMIA SOCIAL.

Entradas para el desarrollo del plan de implementación

Como lo establecen los requerimientos del proceso : “Para la definición del plan de implementación de gestión de seguridad se tomarán como entradas los resultados obtenidos de las etapas de análisis GAP y la definición del plan de tratamiento de riesgos de seguridad de la información.”

Dentro del análisis GAP realizado a la situación actual de la seguridad de la información se estableció el grado de cumplimiento de cada uno de los ítems de la norma ISO 27002, cada ítem fue calificado de acuerdo con la siguiente escala:

ESCALA DE CUMPLIMIENTO
Optimizable
Administrable y medible
Definidos
Repetible pero intuitivo
Inicial / Adhoc
No existe control definido

Los resultados de la evaluación se consolidaron en la declaración de aplicabilidad del SGSI para determinar, que controles se deben aplicar y que controles se deben excluir porque no son aplicables a la entidad.

Para definir el plan de tratamiento de riesgos se siguió la directriz de la norma ISO 27001:2005 en lo referente a:

4.2.1 f) Identificar y evaluar las opciones para el tratamiento de los riesgos.

Las posibles opciones incluyen:

- Aplicar los controles apropiados
- Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos
- Evitar riesgos y
- Transferir a otras partes los riesgos asociados con el negocio.

14.2 Desarrollo del Plan De Implementación Del SGSI

En las matrices de riesgos analizadas para los activos del INSTITUTO PARA LA ECONOMIA SOCIAL, la herramienta define una las 4 opciones posibles para el manejo de cada riesgo: Asumir, Reducir, Evitar y Compartir o Transferir el riesgo. Una vez se determinó la opción de manejo de los riesgos, se describieron las acciones, los responsables y cronograma sugerido para cada una de las acciones de cada uno de los riesgos (ver matrices de riesgos de activos de información desarrolladas por la consultoría para el INSTITUTO PARA LA ECONOMIA SOCIAL).

Para establecer un orden al INSTITUTO PARA LA ECONOMIA SOCIAL sobre el plan de implementación de acuerdo a los dominios de la norma ISO 27001:2005, se recomienda el siguiente orden de ejecución de los planes de implementación de los diferentes dominios.

Orden	Dominio	Observaciones generales
1	A.5 Política de seguridad de la información	Estudiar, ajustar, aprobar y adoptar el documento de políticas de seguridad de la información.
2	A.6 Organización de la seguridad de la información	Activar el [comité de sistemas o el comité que defina el INSTITUTO PARA LA ECONOMIA SOCIAL], y nombrar el [oficial o encargado de seguridad de la información].
3	A.7 Gestión de activos	Inventariar, clasificar y valorar a la mayor brevedad posible la información del INSTITUTO PARA LA ECONOMIA SOCIAL.
4	A.8 Seguridad de los recursos humanos	Realizar las campañas de toma de conciencia en seguridad de la información, actualizar los acuerdos de confidencialidad para que incluyan explícitamente la inclusión de parámetros de seguridad de la información de acuerdo al tipo de persona, contratista y contrato.
5	A.11 Control de acceso	Fortalecer todos los mecanismos de control de acceso de las aplicaciones, implementar una solución de auditoría a las actividades realizadas por los usuarios en los sistemas de información.
6	A.13 Gestión de incidentes de seguridad de la información	Adoptar el procedimiento de gestión de incidentes de seguridad de la información y formar responsables en la atención de los incidentes.

Orden	Dominio	Observaciones generales
7	A.10 Gestión de las comunicaciones	Adoptar mecanismos de cifrado de datos para la información sensible que así lo requiera, de acuerdo al esquema de clasificación de la información. Implementar sistemas centralizados de monitoreo de la infraestructura de TI.
8	A.14 Gestión de la continuidad del negocio	Desarrollar un proyecto de continuidad de negocio para el INSTITUTO PARA LA ECONOMIA SOCIAL.
9	A.12 Adquisición, desarrollo y mantenimiento de software	Adoptar una metodología de desarrollo de software formal con herramientas que faciliten el control y seguimiento de las diferentes etapas del desarrollo.
10	A.15Cumplimiento	Adquisición de herramienta automatizada de análisis de registros de actividades de los usuarios sobre los sistemas de información.
11	A.9 Seguridad física y del entorno	Realizar campaña de toma de conciencia en los usuarios, sobre los riesgos que corren cuando no cumplen o no aplican los controles de acceso físico a las oficinas y la información sensible para la entidad puede quedar expuesta a personal no autorizado.

14.3 Acciones particulares a seguir

Política de seguridad de la información

Actividad	Responsable	Fecha prevista
Revisión y aprobación de la política de seguridad del SGSI del INSTITUTO PARA LA ECONOMIA SOCIAL.	Comité de sistemas o el que defina la entidad.	Julio 2013
Revisión y aprobación de políticas complementarias a la seguridad de la información	Comité de sistemas o el que defina la entidad.	Julio 2013

Actividad	Responsable	Fecha prevista
Ejecución de actividades de toma de conciencia en seguridad de la información	Sistema integrado de gestión	Segundo semestre 2013 septiembre
Evaluación de nivel de apropiación de la política de seguridad de la información (pruebas de ingeniería social)	Contrato con tercero	Octubre 2013

Organización de la seguridad de la información

Actividad	Responsable	Fecha prevista
Activar el comité de sistemas o el comité que designe el INSTITUTO PARA LA ECONOMIA SOCIAL y definir la periodicidad de las reuniones.	Dirección del INSTITUTO PARA LA ECONOMIA SOCIAL.	Julio 2013
Incluir dentro de las entradas para la revisión de la dirección del SGSI: política de seguridad de la información, estado de incidentes de seguridad de la información, cambios en la normatividad sobre la seguridad de la información.	Sistema integrado de gestión	Julio 2013
Documentar o consolidar la documentación de instrucciones de trabajo para la operación de los componentes de infraestructura de IT. Desarrollar manuales de responsabilidades detalladas para los administradores de los sistemas de información que incluyan las tareas específicas que debe desarrollar cada profesional para la operación de los sistemas a su cargo.	Área de sistemas y administradores de los sistemas de información misional	Segundo semestre 2013
Elaborar material de inducción sobre aspectos de seguridad de la información para todas las personas que sean vinculadas al INSTITUTO PARA LA ECONOMIA SOCIAL. Generar una presentación de computador que puede publicarse en la intranet para consulta obligatoria del personal que ingresa a laborar al INSTITUTO PARA LA ECONOMIA SOCIAL.	Cada proceso misional	Segundo semestre 2013 Agosto

Actividad	Responsable	Fecha prevista
Incluir dentro del proceso de inducción a contratistas la presentación de la sensibilización de la seguridad de la información.		
Formalizar el establecimiento de análisis de riesgos de seguridad de la información cuando se quieren habilitar nuevos servicios de procesamiento de datos.	Comité de sistemas o el que defina la entidad.	Agosto 2013
Delegar en el área de contratos la formalización del acuerdo de confidencialidad.	Área jurídica y de Contratos	Agosto 2013
Definir un rol como [oficial o encargado de seguridad de la información].	Comité de sistemas o el que defina la entidad.	Julio 2013

Gestión de activos

Actividad	Responsable	Fecha prevista
Aprobación de los niveles de clasificación de la información.	Comité de sistemas o el que defina la entidad.	Julio 2013
Determinar la viabilidad de utilizar las etiquetas de metadatos para los documentos generados por los usuarios. Verificar con gestión documental si están aplicando o exigiendo a los usuarios la aplicación del nivel de seguridad a los documentos.	Sistema de gestión documental	Segundo semestre 2013
Desarrollo de base datos para inventario y clasificación de información	Área de Sistemas	Primer semestre 2014

Seguridad de los recursos humanos

Actividad	Responsable	Fecha prevista

Actividad	Responsable	Fecha prevista
Elaboración de código de conducta sobre seguridad de la información	Comité de sistemas o el que defina la entidad.	Segundo semestre 2013
Elaboración de planes de capacitación y toma de conciencia en seguridad de la información.	Área de sistemas	Segundo semestre 2013
Determinar con el área de control interno disciplinario las condiciones a cumplir para iniciar una investigación administrativa por incidentes de seguridad de la información	Área de control interno	Agosto 2013
Incluir dentro de los contratos clausulas sobre incumplimiento de la ley 1273 de 2009, “Delitos informáticos”	Área jurídica / contratos	Agosto 2013

Control de acceso

Actividad	**Responsable**	**Fecha prevista**
Aprobación y adopción de política de acceso a sistemas de información.	Comité de sistemas o el que defina la entidad.	Julio 2013
Definición, aprobación y adopción de política de uso de equipos móviles	Comité de sistemas o el que defina la entidad.	Julio. 2013
Evaluación de compra de equipo para registro de auditoría sobre acceso a sistemas de información	Área de sistemas	Octubre. 2013

Gestión de incidentes de seguridad de la información

Actividad	**Responsable**	**Fecha prevista**
Aprobación y adopción de procedimiento de manejo de incidentes de seguridad de la información (difusión a mesa de ayuda y demás colaboradores del INSTITUTO PARA	Comité de sistemas o el que defina la entidad.	Sep. 2013

Actividad	Responsable	Fecha prevista
LA ECONOMIA SOCIAL)		
Selección y nombramiento del [oficial o encargado de seguridad de la información]	Comité de sistemas o el que defina la entidad.	Julio 2013
Preparación de primeros respondientes en incidentes de seguridad de la información	Comité de sistemas o el que defina la entidad.	Segundo semestre 2013
Evaluación de compra de herramienta de auditoría a accesos a sistemas de información	Área de sistemas y Área de control interno	Octubre. 2013

Gestión de comunicaciones

Actividad	Responsable	Fecha prevista
Complementar y completar la Documentación de procedimientos de operación de sistemas y dispositivos de TI.	Área de sistemas	Segundo semestre 2013
Incluir el análisis de riesgos en cualquier proceso de atención de requerimientos.	Área de sistemas	Segundo semestre 2013
Implementar un procedimiento de control de cambios para TI.	Área de sistemas	Oct. 2013
Elaborar una lista de chequeo sobre la utilización de los ambientes de pruebas y paso de cambios de TI a producción (ej. 1. evaluación de cambio aprobada. 2 Protocolo de pruebas del cambio documentado. 3 respaldo de datos del ambiente de pruebas ejecutado. 4 responsables del cambio identificados. Etc.)	Área de sistemas	Oct. 2013
Evaluar la posibilidad de implementar una consola única de monitoreo y registro de eventos y reportes de los equipos de IT (opciones: CA Unicenter, Nagios, Tivoli)	Área de sistemas	Octubre. 2013
De acuerdo a los niveles de clasificación de	Área de sistemas y	Octubre 2013

Actividad	Responsable	Fecha prevista
la información, evaluar la necesidad de cifrar backup que salen de la entidad y correos electrónicos de usuarios con acceso a información sensible de la entidad.	procesos misionales	
Definición de la política de destrucción de cintas de respaldo de datos que cumplan su vida útil. Coordinación con el área de activos fijos para formalizar la legalidad del procedimiento de destrucción de elementos consumibles	Área de sistemas, Área administrativa	Nov. 2013
Implementación formal de software de borrado seguro	Área de sistemas	Octubre. 2013
Ejecución de inventario de información y clasificación de los mismos	Área de sistemas	Dic. 2013
Estudiar la implementación de filtrado de archivos adjuntos en los correos electrónicos institucionales de acuerdo con su contenido.	Área de sistemas	Octubre. 2013

Gestión de continuidad del negocio

Actividad	Responsable	Fecha prevista
Desarrollo del Análisis de impacto al negocio (realizar talleres con los procesos misionales para identificar los procesos críticos)	Comité de sistemas o el que defina la entidad.	Primer semestre 2014
Desarrollo de talleres de gestión de riesgo (identificar los escenarios de riesgo que pueden paralizar los procesos críticos)	Comité de sistemas o el que defina la entidad.	Primer semestre 2014
Desarrollo de las estrategias para garantizar la continuidad de las actividades de negocio	Comité de sistemas o el que defina la entidad.	Primer semestre 2014
Desarrollo de los procedimientos detalladas para las actividades de continuidad de negocio	Comité de sistemas o el que defina la entidad.	Primer semestre 2014
Prueba del plan de continuidad de negocio	Comité de sistemas o el que defina la	Primer semestre

Actividad	Responsable	Fecha prevista
	entidad.	2014
Mantenimiento del plan de continuidad de negocio	Comité de sistemas o el que defina la entidad.	Primer semestre 2014

Adquisición desarrollo y mantenimiento de software

Actividad	Responsable	Fecha prevista
Aprobación e implementación de política de control de cifrado de datos	Comité de sistemas o el que defina la entidad.	Noviembre 2013
Selección de herramienta (software o procedimiento) para la administración de llaves de cifrado de datos	Comité de sistemas o el que defina la entidad.	Noviembre 2013
Evaluación de compra de herramienta de auditoría a uso de sistemas de información	Área de sistemas	Octubre 2013
Implementación procedimiento de manejo de incidentes de seguridad de la información	Área de sistemas	Agosto 2013

Cumplimiento

Actividad	Responsable	Fecha prevista
Actualizar la lista de normatividad de seguridad de la información aplicable INSTITUTO PARA LA ECONOMIA SOCIAL	Área de Sistemas, Área Jurídica	Agosto 2013
Mejoramiento de controles para mantenimiento y transporte de carpetas y archivos de los procesos misionales.	Gestión documental	Dic. 2013
Adopción de la política de uso de controles de cifrado de datos	Comité de sistemas o el que defina la entidad.	Julio 2013

Actividad	Responsable	Fecha prevista
Evaluación de adquisición de equipo de auditoría sobre actividades en sistemas de información	Área de sistemas	Octubre. 2013

Seguridad física y de entorno

Actividad	Responsable	Fecha prevista
Desarrollo de planes de toma de conciencia en seguridad de la información	Sistema integrado de gestión	Segundo semestre 2013 Septiembre
Evaluación del protocolo de acompañamiento de visitantes en las instalaciones del INSTITUTO PARA LA ECONOMIA SOCIAL	Comité de sistemas o el que defina la entidad.	Septiembre 2013
Aprobación de política de pantalla limpia y escritorio despejado	Comité de sistemas o el que defina la entidad.	Julio 2013
Implementar cantoneras para control de acceso a las oficinas de la entidad	Área administrativa	Primer semestre 2014

15 CONTROLES SELECCIONADOS DEL SGSI:

En la siguiente tabla (tabla 1), se encuentran los controles seleccionados del Subsistema de Gestión de Seguridad de la Información del IPES.

Tabla 1. Controles Seleccionados IPES.

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
5	POLÍTICA DE SEGURIDAD		
5.1	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
5.1.1	DOCUMENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SI	Obligación normativa de la Comisión Distrital de Sistemas: Resolución 305 de 2008
5.1.2	REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SI	Obligación normativa de la Comisión Distrital de Sistemas: Resolución 305 de 2008
		2	
6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION		
6.1	ORGANIZACIÓN INTERNA		
6.1.1	COMPROMISO DE LA DIRECCIÓN CON LA SEGURIDAD DE LA INFORMACIÓN	SI	Requerimiento normativo de la Alcaldía Mayor de Bogotá, Decreto 651 de 2011
6.1.2	COORDINACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	SI	Obligación normativa de la Comisión Distrital de Sistemas: Resolución 305 de 2008
6.1.3	ASIGNACIÓN DE RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	Obligación normativa de la Comisión Distrital de Sistemas: Resolución 305 de 2008
6.1.4	PROCESOS DE AUTORIZACIÓN PARA LOS SERVICIOS DE PROCESAMIENTO DE INFORMACIÓN	SI	Obligación normativa de la Comisión Distrital de Sistemas: Resolución 305 de 2008
6.1.5	ACUERDOS DE CONFIDENCIALIDAD	SI	Mecanismos de control para dar cumplimiento al Código contencioso administrativo y la ley de protección de datos personales
6.1.6	CONTACTO CON LAS AUTORIDADES	SI	Obligación normativa de la Comisión Distrital de Sistemas: Resolución 305 de 2008
6.1.7	CONTACTO CON GRUPOS DE INTERÉS ESPECIALES	SI	Obligación normativa de la Comisión Distrital de Sistemas: Resolución 305 de 2008
6.1.8	REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	SI	Obligación normativa derivada del Modelo Estándar de Control Internos para la entidades del estado
6.2	PARTES EXTERNAS		

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
6.2.1	IDENTIFICACIÓN DE LOS RIESGOS RELACIONADOS CON LAS PARTES EXTERNAS	SI	Obligación normativa de la Comisión Distrital de Sistemas: Resolución 305 de 2008
6.2.2	CONSIDERACIONES DE LA SEGURIDAD CUANDO SE TRATA CON LOS CLIENTES	SI	Obligación derivada de la Norma Técnica Distrital "Sistema Integrado de Gestión"
6.2.3	CONSIDERACIONES DE LA SEGURIDAD EN LOS ACUERDOS CON TERCERAS PARTES	SI	Obligación derivada de la Norma Técnica Distrital "Sistema Integrado de Gestión", El modelo estándar de control Interno para entidades estatales.
		11	
7	GESTION DE ACTIVOS		
7.1	RESPONSABILIDAD POR LOS ACTIVOS		
7.1.1	INVENTARIO DE ACTIVOS.	SI	Requerimiento del Subsistema Gestión de Seguridad de la Información del IPES, soportado en la Norma Técnica Distrital "Sistema Integrado de Gestión" y la resolución 305 de 2008 de la Comisión Distrital de Sistemas
7.1.2	PROPIEDAD DE LOS ACTIVOS	SI	Control del Subsistema de gestión de seguridad de la Información para mitigar los riesgos identificados.
7.1.3	USO ACEPTABLE DE LOS ACTIVOS	SI	Obligación normativa de la Comisión Distrital de Sistemas: Resolución 305 de 2008, "POLITICAS GENERALES DE TECNOLOGIA DE INFORMACION Y COMUNICACIONES APLICABLES A LAS ENTIDADES DEL DISTRITO CAPITAL "
7.2	CLASIFICACIÓN DE LA INFORMACIÓN		
7.2.1	DIRECTRICES DE CLASIFICACIÓN	SI	Obligación normativa derivada de la implementación del Programa Integral de gestión de archivo, control necesario para mitigar los riesgos de divulgación de información personal sensible ley 1581 de 2012
7.2.2	ETIQUETADO Y MANEJO DE LA INFORMACION	SI	Control para lograr la identificación de la información gestionada por los diversos procesos misionales y mitigar los riesgos de divulgación de información reservada o sensible personal, ley 1581 de 2012
		5	

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
8	SEGURIDAD DE LOS RECURSOS HUMANOS		
8.1	ANTES DEL EMPLEO		
8.1.1	ROLES Y RESPONSABILIDADES	SI	Requisito del Departamento Administrativo de la Función Pública
8.1.2	SELECCIÓN	SI	Requerimientos normativos de contracción de personal en la entidades Distritales
8.1.3	TERMINOS Y CONDICIONES LABORALES	SI	Requerimientos normativos de contratación de personal en la entidades Distritales
8.2	DURANTE LA VIGENCIA DE LA CONTRATACIÓN LABORAL		
8.2.1	RESPONSABILIDADES DE LA DIRECCIÓN	SI	Obligación normativa de la Norma Técnica Distrital Sistema Integrado de Gestión y la resolución 305 de 2008 de la Comisión Distrital de Sistemas
8.2.2	EDUCACIÓN, FORMACIÓN Y CONCIENTIZACIÓN SOBRE LA SEGURIDAD DE LA INFORMACIÓN	SI	Control requerido por el Subsistema de gestión de seguridad de la información del IPES para mitigar los riesgos de seguridad de la información
8.2.3	PROCESO DISCIPLINARIO	SI	Obligación normativa de la Procuraduría General de la Nación Código Disciplinario Único ley 734 de 2002
8.3	TERMINACIÓN O CAMBIO DE LA CONTRATACIÓN LABORAL		
8.3.1	RESPONSABILIDADES EN LA TERMINACIÓN	SI	Requerimientos normativos de contratación de personal en la entidades Distritales
8.3.2	DEVOLUCIÓN DE LOS ACTIVOS	SI	Requerimientos normativos de contratación de personal en la entidades Distritales
8.3.3	RETIRO DE LOS DERECHOS DE ACCESO	SI	Control requerido por el Subsistema de gestión de seguridad de la información del IPES para mitigar los riesgos de seguridad de la información generados por el acceso a sistemas de información por parte de contratistas y funcionarios cuando cesan sus funciones
		9	
9	SEGURIDAD FISICA Y DEL ENTORNO		

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
9.1	AREAS SEGURAS		
9.1.1	ÁREAS DE SEGURIDAD FÍSICA	SI	Control requerido por el subsistema de gestión de seguridad de la información para proteger los activos de información de acceso no autorizado de personal externo al IPES
9.1.2	CONTROLES DE ACCESO FÍSICO.	SI	Control requerido por el subsistema de gestión de seguridad de la información para proteger los activos de información de acceso no autorizado de personal externo al IPES
9.1.3	SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	SI	Control requerido por el subsistema de gestión de seguridad de la información para proteger los activos de información de acceso no autorizado de personal externo al IPES
9.1.4	PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	SI	Control requerido por el subsistema de gestión de seguridad de la información para proteger los activos de información de acceso no autorizado de personal externo al IPES
9.1.5	TRABAJO EN ÁREAS SEGURAS	SI	Control requerido por el subsistema de gestión de seguridad de la información para proteger los activos de información de acceso no autorizado de personal externo al IPES
9.1.6	ÁREAS DE CARGA, DESPACHO Y ACCESO PÚBLICO	SI	Control requerido por el subsistema de gestión de seguridad de la información para proteger los activos de información de acceso no autorizado de personal externo al IPES
9.2	SEGURIDAD DE LOS EQUIPOS		
9.2.1	UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	SI	Control requerido por el subsistema de gestión de seguridad de la información para proteger los activos de información de daños generados por condiciones ambientales y amenazas externas como personal no autorizado
9.2.2	SERVICIOS DE SUMINISTRO	SI	Control requerido por el subsistema de gestión de seguridad de la información para mitigar los riesgos generados por fallas en el suministro de fluido eléctrico

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
9.2.3	SEGURIDAD DE CABLEADO	SI	Control requerido por el subsistema de gestión de seguridad de la información para mitigar los riesgos generados por acceso no autorizado al cableado de red del IPES
9.2.4	MANTENIMIENTO DE LOS EQUIPOS	SI	Control requerido por el subsistema de gestión de seguridad de la información para mitigar los riesgos generados por fallas en los equipos de procesamiento de datos del IPES, control derivado de los planes operativos anuales del IPES
9.2.5	SEGURIDAD DE LOS EQUIPOS FUERAS DE LAS INSTALACIONES	SI	Control requerido por el subsistema de gestión de seguridad de la información del IPES para mitigar los riesgos de pérdida de información en equipos portátiles de la Entidad
9.2.6	SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE LOS EQUIPOS	SI	Control requerido por el Subsistema de gestión de seguridad de la información para evitar la divulgación no autorizada de información cuando se reasigna un computador a otro funcionario o contratista o cuando se da de baja un equipo por daño u obsolescencia
9.2.7	RETIRO DE ACTIVOS	SI	Requisito de control de activos e inventarios del IPES
		13	
10	GESTIÓN DE COMUNICACIONES Y OPERACIONES		
10.1	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES		
10.1.1	DOCUMENTACIÓN DE LOS PROCEDIMIENTOS DE OPERACIÓN	SI	Requerimiento normativo derivado de la implementación de la Norma NTC-GP1000 y el Sistema Integrado de Gestión Distrital
10.1.2	GESTIÓN DEL CAMBIO	SI	Control seleccionado para mitigar los riesgos generados por posibles cambios en la infraestructura tecnológica del IPES que no se controlan mediante documentación formal.
10.1.3	DISTRIBUCIÓN DE FUNCIONES	SI	Control derivado de las asignaciones de roles y responsabilidades asignadas en el manual de funciones de cada funcionario y las obligaciones contractuales del personal por prestación de servicios

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
10.1.4	SEPARACIÓN DE LAS INSTALACIONES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN	SI	Control seleccionado para mitigar errores en el paso a producción de paquetes de software no probados
10.2	GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR TERCERAS PARTES		
10.2.1	PRESTACIÓN DEL SERVICIO	SI	Requisito derivado de las políticas de seguridad de la información de la comisión distrital de sistemas, resolución 305 de 2008
10.2.2	MONITOREO Y REVISIÓN DE LOS SERVICIOS POR TERCERAS PARTES	SI	Obligación legal derivada de las actividades de supervisión de contratos establecida por el modelo de contratación distrital y nacional. Control implementado para mitigar los riesgos derivados de la contratación de servicios a un tercero.
10.2.3	GESTIÓN DE LOS CAMBIOS EN LOS SERVICIOS POR TERCERAS PARTES	SI	Control del subsistema de gestión de seguridad de la información para controlar los riesgos generados por cambios no controlados en los servicios y activos de información
10.3	PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA		
10.3.1	GESTIÓN DE LA CAPACIDAD	SI	Control seleccionado para mitigar riesgos de pérdida de disponibilidad de los servicios informáticos y como insumo para los procesos de planificación estratégica de los sistemas de información.
10.3.2	ACEPTACIÓN DEL SISTEMA	SI	Control implementado para dar cumplimiento a las obligaciones de supervisión de contratos de prestación de servicios informáticos y control de la aceptación de cambios solicitados por los usuarios a los sistemas de información del IPES
10.4	PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y MÓVILES		
10.4.1	CONTROLES CONTRA CÓDIGO MALICIOSOS	SI	Control para mitigar las amenazas generadas por el malware
10.4.2	CONTROLES CONTRA CÓDIGOS MÓVILES	NO	Los sistemas de información del IPES no emplean códigos móviles, la arquitectura de desarrollo basada en .NET controla la utilización de código móvil.
10.5	RESPALDO		

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
10.5.1	RESPALDO DE LA INFORMACIÓN	SI	La resolución 305 de 2008 de la Comisión Distrital de sistemas obliga al establecimiento de una política y procedimientos de respaldo de información. Las buenas prácticas de administración de sistemas informáticos recomiendan el uso de copias de respaldo como mecanismo de recuperación ante fallas de sistemas informáticos
10.6	GESTIÓN DE LA SEGURIDAD DE LAS REDES		
10.6.1	CONTROLES DE LAS REDES	SI	Control establecido para impedir amenazas generadas por atacantes informáticos
10.6.2	SEGURIDAD DE LOS SERVICIOS DE LA RED	SI	Control establecido para impedir amenazas generadas por atacantes informáticos
10.7	MANEJO DE LOS MEDIOS		
10.7.1	GESTIÓN DE LOS MEDIOS REMOVIBLES	SI	2. Requerimiento de seguridad de la información de la Norma ISO27001, control seleccionado para mitigar el riesgo de pérdida de información por medios removibles
10.7.2	ELIMINACIÓN DE LOS MEDIOS	SI	2. Requerimiento de seguridad de la información de la Norma ISO27001, control seleccionado para mitigar el riesgo de pérdida o divulgación de información en medios de almacenamiento dados de baja
10.7.3	PROCEDIMIENTO PARA EL MANEJO DE LA INFORMACIÓN	SI	Control implementado para dar cumplimiento a la normatividad de información personal y requerimientos del procedimiento contencioso administrativo
10.7.4	SEGURIDAD DE LA DOCUMENTACIÓN DEL SISTEMA	SI	Control establecido para impedir amenazas generadas por atacantes informáticos
10.8	INTERCAMBIO DE LA INFORMACIÓN		
10.8.1	POLÌTICAS Y PROCEDIMIENTOS PARA EL INTERCAMBIO DE LA INFORMACIÓN	SI	Control implementado para mitigar los riesgos generados por la divulgación de información institucional o de datos personales cuando se deben intercambiar con otras entidades nacionales o distritales
10.8.2	ACUERDOS PARA EL INTERCAMBIO	SI	Control implementado para mitigar los riesgos generados por la divulgación de información institucional o de datos personales cuando se deben intercambiar con otras entidades nacionales o

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
			distritales
10.8.3	MEDIOS FÍSICOS EN TRANSITO	SI	Control implementado para mitigar los riesgos generados por la divulgación de información institucional o de datos personales cuando se deben intercambiar con otras entidades nacionales o distritales
10.8.4	MENSAJERIA ELECTRÓNICA	SI	Requerimiento normativo establecido por la resolución 305 de 2008 de la comisión Distrital de Sistemas
10.8.5	SISTEMAS DE INFORMACIÓN DEL NEGOCIO	SI	Control implementado para mitigar los riesgos generados por la divulgación de información institucional o de datos personales cuando se deben intercambiar con otras entidades nacionales o distritales o se brinda acceso al ciudadano a información institucional
10.9	SERVICIOS DE COMERCIO ELECTRÓNICO		
10.9.1	COMERCIO ELECTRÓNICO	NO	EL IPES no realiza operaciones de comercio electrónico, la entidad no comercializa bienes o servicios empleando medios electrónicos
10.9.2	TRANSACCIONES EN LÍNEA	NO	EL IPES no realiza operaciones de comercio electrónico, la entidad no comercializa bienes o servicios empleando medios electrónicos
10.9.3	INFORMACIÓN DISPONIBLE AL PUBLICO	NO	EL IPES no realiza operaciones de comercio electrónico, la entidad no comercializa bienes o servicios empleando medios electrónicos
10.10	MONITOREO		
10.10.1	REGISTRO DE AUDITORÍAS	SI	Requerimiento normativo derivado de la implementación de la Norma NTC-GP1000 y el Sistema de control Interno MECI1000
10.10.2	MONITOREO DEL USO DEL SISTEMA	SI	Requerimiento normativo derivado de la implementación de la Norma NTC-GP1000 y el Sistema de control Interno MECI1000 y los procedimientos de administración y mantenimiento de los sistemas informáticos del IPES

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
10.10.3	PROTECCIÓN DE LA INFORMACIÓN DE LOGS	SI	Requerimiento normativo derivado de la implementación de la Norma NTC-GP1000 y el Sistema de control Interno MECI1000 y los procedimientos de administración y mantenimiento de los sistemas informáticos del IPES
10.10.4	REGISTRO DEL ADMINISTRADOR Y DEL OPERADOR	SI	Requerimiento normativo derivado de la implementación de la Norma NTC-GP1000 y el Sistema de control Interno MECI1000 y los procedimientos de administración y mantenimiento de los sistemas informáticos del IPES
10.10.5	REGISTRO DE FALLAS	SI	Requerimiento normativo derivado de la implementación de la Norma NTC-GP1000 y el Sistema de control Interno MECI1000 y los procedimientos de administración y mantenimiento de los sistemas informáticos del IPES
10.10.6	SINCRONIZACIÓN DE RELOJES	SI	Requerimiento legal derivado del uso de la hora oficial colombiana. "De acuerdo con lo establecido en el numeral 14 del artículo 6 del Decreto número 4175 de 2011 del Ministerio de Comercio Industria y Turismo, el Instituto Nacional de Metrología mantiene, coordina y difunde la hora legal de la República de Colombia." El control permite la sincronización de los relojes de servidores y sus respectivos logs.
		28	
11	CONTROL DE ACCESO		
11.1	REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO		
11.1.1	POLÍTICA DE CONTROL DE ACCESO	SI	Control implementado para dar cumplimiento a la resolución 305 de 2008 de la comisión Distrital de Sistemas y para mitigar riesgos de acceso no autorizado a sistemas de información
11.2	GESTIÓN DEL ACCESO A USUARIOS		
11.2.1	REGISTRO DE USUARIOS	SI	Requerimiento del subsistema de gestión de seguridad de la información IPES para mitigar el acceso no autorizado a sistemas de información
11.2.2	GESTIÓN DE PRIVILEGIOS	SI	Requerimiento del subsistema de gestión de seguridad de la información IPES para mitigar el acceso no autorizado a sistemas de información

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
11.2.3	GESTIÓN DE CONTRASEÑAS PARA USUARIOS	SI	Control adoptado como buena práctica para el control de acceso a sistemas de información
11.2.4	REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS	SI	Requerimiento generado de los controles de seguridad para auditar sistemas de información de acuerdo con los requisitos del MECI1000
11.3	RESPONSABILIDADES DE LOS USUARIOS		
11.3.1	USO DE CONTRASEÑAS	SI	Control adoptado como buena práctica para el control de acceso a sistemas de información
11.3.2	EQUIPOS DE USUARIO DESATENDIDO	SI	Control adoptado para mitigar riesgos de acceso a información por parte de personal no autorizado
11.3.3	POLÍTICA DE ESCRITORIO DESPEJADO Y DE PANTALLA DESPEJADA	SI	Control adoptado para mitigar riesgos de acceso a información por parte de personal no autorizado
11.4	CONTROL DE ACCESO A LAS REDES		
11.4.1	POLÍTICA DEL USO DE LOS SERVICIOS DE RED	SI	Control implementado para dar cumplimiento a la resolución 305 de 2008 de la comisión Distrital de Sistemas y para mitigar riesgos de acceso no autorizado a sistemas de información
11.4.2	AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS	SI	Control implementado para dar cumplimiento a la resolución 305 de 2008 de la comisión Distrital de Sistemas y para mitigar riesgos de acceso no autorizado a sistemas de información
11.4.3	IDENTIFICACIÓN DE LOS EQUIPOS EN LAS REDES	SI	Control implementado como mecanismo de auditabilidad de las acciones realizadas desde estaciones de trabajo
11.4.4	PROTECCIÓN DE LOS PUERTOS DE CONFIGURACIÓN Y DIAGNÓSTICO REMOTO	SI	Control implementado para mitigar riesgos generados por atacantes externos
11.4.5	SEPARACIÓN DE LAS REDES	SI	Control implementado para mitigar riesgos generados por atacantes externos o internos
11.4.6	CONTROL DE CONEXIÓN DE LAS REDES	SI	Control implementado para mitigar riesgos generados por atacantes externos o internos
11.4.7	CONTROL DE ENRUTAMIENTO EN LA RED	SI	Control implementado para mitigar riesgos generados por atacantes externos o internos
11.5	CONTROL DE ACCESO AL SISTEMA OPERATIVO		

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
11.5.1	PROCEDIMIENTO DE INGRESO SEGURO	SI	Control implementado para mitigar riesgos generados por atacantes externos o internos
11.5.2	IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS	SI	Control adoptado como buena práctica para el control de acceso a sistemas de información y sistemas operacionales
11.5.3	SISTEMA DE GESTIÓN DE CONTRASEÑAS	SI	Control adoptado como buena práctica para el control de acceso a sistemas de información y sistemas operacionales
11.5.4	USO DE LAS UTILIDADES DEL SISTEMA	SI	Control implementado para mitigar riesgos generados por atacantes externos o internos
11.5.5	TIEMPO DE INACTIVIDAD DE LA SESION	SI	Control implementado para fortalecer la política de escritorio y pantalla despejadas
11.5.6	LIMITACIÓN DEL TIEMPO DE CONEXIÓN	SI	Control implementado para mitigar riesgos generados por atacantes externos o internos
11.6	CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN		
11.6.1	RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	SI	Control implementado para mitigar los riesgos de acceso no autorizado a información clasificada como reservada, estratégica o sensible personal
11.6.2	AISLAMIENTO DE SISTEMAS SENSIBLES	SI	Control implementado para mitigar los riesgos de acceso no autorizado a información clasificada como reservada, estratégica o sensible personal
11.7	COMPUTACIÓN MÓVIL		
11.7.1	COMPUTACIÓN Y COMUNICACIONES MÓVILES	SI	Control implementado para permitir la política gubernamental de teletrabajo. Decreto 0884 de 2012 - Vive Digital
11.7.2	TRABAJO REMOTO	SI	Control implementado para permitir la política gubernamental de teletrabajo. Decreto 0884 de 2012 - Vive Digital
		25	
12	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION		
12.1	REQUISICIÓN DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN		
12.1.1	ANÁLISIS Y ESPECIFICACIÓN DE LOS REQUERIMIENTOS DE SEGURIDAD	SI	Requerimiento de la resolución 305 de 2008 de la Comisión Distrital de Sistemas. Implementación de la seguridad de la información en el desarrollo de sistemas de información

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
12.2	PROCESAMIENTO CORRECTO EN LAS APLICACIONES		
12.2.1	VALIDACIÓN DE LOS DATOS DE ENTRADA	SI	Requerimiento de la resolución 305 de 2008 de la Comisión Distrital de Sistemas. Implementación de la seguridad de la información en el desarrollo de sistemas de información
12.2.2	CONTROL DE PROCESAMIENTO INTERNO	SI	Requerimiento de la resolución 305 de 2008 de la Comisión Distrital de Sistemas. Implementación de la seguridad de la información en el desarrollo de sistemas de información. Mecanismo de auditabilidad de los sistemas de información para facilitar la implementación de controles del MECI1000
12.2.3	INTEGRIDAD DEL MENSAJE	SI	Requerimiento de seguridad de la información
12.2.4	VALIDACIÓN DE LOS DATOS DE SALIDA	SI	Requerimiento de la resolución 305 de 2008 de la Comisión Distrital de Sistemas. Implementación de la seguridad de la información en el desarrollo de sistemas de información. Mecanismo de auditabilidad de los sistemas de información para facilitar la implementación de controles del MECI1000
12.3	CONTROLES CRIPTOGRAFICOS		
12.3.1	POLÍTICAS SOBRE EL USO DE CONTROLES CRIPTOGRAFICOS	SI	Control para la protección de la información clasificada como personal sensible y reservada almacenada fuera de los sistemas de información
12.3.2	GESTIÓN DE LLAVES	SI	Requerimiento de seguridad del subsistema de gestión de seguridad de la información del IPES
12.4	SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA		
12.4.1	CONTROL DEL SOFTWARE OPERATIVO	SI	Mecanismo de seguridad para mitigar los riesgos generados por atacantes externos o internos

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
12.4.2	PROTECCIÓN DE LOS DATOS DE PRUEBA DEL SISTEMA	SI	Requerimiento de la resolución 305 de 2008 de la Comisión Distrital de Sistemas. Implementación de la seguridad de la información en el desarrollo de sistemas de información. Mecanismo de auditabilidad de los sistemas de información para facilitar la implementación de controles del MECI1000
12.4.3	CONTROL DE ACCESO A LOS CÓDIGO FUENTE DE LOS PROGRAMAS	SI	Requerimiento de la resolución 305 de 2008 de la Comisión Distrital de Sistemas. Implementación de la seguridad de la información en el desarrollo de sistemas de información. Mecanismo de auditabilidad de los sistemas de información para facilitar la implementación de controles del MECI1000
12.5	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE		
12.5.1	PROCEDIMIENTOS DE CONTROL DE CAMBIOS	SI	Requerimiento de la resolución 305 de 2008 de la Comisión Distrital de Sistemas. Implementación de la seguridad de la información en el desarrollo de sistemas de información. Mecanismo de auditabilidad de los sistemas de información para facilitar la implementación de controles del MECI1000
12.5.2	REVISIÓN TÉCNICA DE LAS APLICACIONES DESPUÉS DE LOS CAMBIOS EN EL SISTEMA OPERATIVO	SI	Requerimiento de la resolución 305 de 2008 de la Comisión Distrital de Sistemas. Implementación de la seguridad de la información en el desarrollo de sistemas de información. Mecanismo de auditabilidad de los sistemas de información para facilitar la implementación de controles del MECI1000
12.5.3	RESTRICCIONES EN CAMBIOS A LOS PAQUETES DE SOFTWARE	SI	Requerimiento de la resolución 305 de 2008 de la Comisión Distrital de Sistemas. Implementación de la seguridad de la información en el desarrollo de sistemas de información. Mecanismo de auditabilidad de los sistemas de información para facilitar la implementación de controles del MECI1000

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
12.5.4	FUGA DE INFORMACIÓN	SI	Control para la protección de la información clasificada como personal sensible y reservada almacenada fuera de los sistemas de información
12.5.5	DESARROLLO DE SOFTWARE CONTRATANDO EXTERNAMENTE	SI	Control implementado para cumplir los requisitos de supervisión de contratos e implementar la seguridad en el ciclo de vida del desarrollo del software según directriz de la resolución 305 de 2008 de la comisión distrital de sistemas
12.6	GESTIÓN DE LA VULNERABILIDAD TÉCNICA		
12.6.1	CONTROL DE VULNERABILIDADES TÉCNICAS	SI	control implementado para identificar las vulnerabilidades que pueden afectar los activos de información y cumplir los requerimientos de gestión de riesgos del subsistema de gestión de seguridad de la información del IPES
		16	
13	GESTIÓN DE INCIDENTES		
13.1	REPORTE SOBRE LOS EVENTOS Y LAS DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN		
13.1.1	REPORTES SOBRE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	SI	Requisito del subsistema de gestión de seguridad de la información del IPES.
13.1.2	REPORTE SOBRE LAS DEBILIDADES DE LA SEGURIDAD	SI	Control que permite detectar las vulnerabilidades que afectan al subsistema de gestión de seguridad de la información de IPES. El control permite identificar las causas de no conformidades potenciales que pueden afectar la seguridad de la información
13.2	GESTIÓN DE LOS INCIDENTES Y LAS MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN		
13.2.1	RESPONSABILIDADES Y PROCEDIMIENTOS	SI	Requisito del subsistema de gestión de seguridad de la información del IPES.
13.2.2	APRENDIZAJE DEBIDO A LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	SI	Requisito del subsistema de gestión de seguridad de la información del IPES.

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
13.2.3	RECOLECCIÓN DE EVIDENCIA	SI	Control seleccionado para recolectar pruebas ante posibles investigaciones administrativas o reporte ante las autoridades competentes en caso de incidentes de seguridad de la información
		5	
14	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
14.1	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN, DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
14.1.1	INCLUSIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	SI	Requerimiento normativo impuesto por la resolución 305 de 2008 de la comisión distrital de sistemas
14.1.2	CONTINUIDAD DEL NEGOCIO Y EVALUACIÓN DE RIESGOS	SI	Requerimiento del subsistema de gestión de seguridad de la información que permite identificar los riesgos que pueden afectar la continuidad en la prestación de los servicios.
14.1.3	DESARROLLO E IMPLEMENTACIÓN DE PLANES DE CONTINUIDAD QUE INCLUYEN LA SEGURIDAD DE LA INFORMACIÓN	SI	Requerimiento normativo impuesto por la resolución 305 de 2008 de la comisión distrital de sistemas
14.1.4	ESTRUCTURA PARA LA PLANIFICACIÓN DE LA CONTINUIDAD DEL NEGOCIO	SI	Requerimiento normativo impuesto por la resolución 305 de 2008 de la comisión distrital de sistemas
14.1.5	PRUEBAS, MANTENIMIENTO Y REEVALUACIÓN DE LOS PLANES DE CONTINUIDAD DEL NEGOCIO	SI	Requerimiento normativo impuesto por la resolución 305 de 2008 de la comisión distrital de sistemas
		5	
15	CUMPLIMIENTO		
15.1	CUMPLIMIENTO DE LOS REQUISITOS LEGALES		
15.1.1	IDENTIFICACIÓN DE LA LEGISTACIÓN APLICABLE	SI	Requisito legal del modelo estándar de control interno MECI1000 y el subsistema de gestión de la calidad de IPES
15.1.2	DERECHOS DE PROPIEDAD INTELECTUAL	SI	Requisito legal impuesto por la legislación Colombiana. Ley de Derechos de autor

ANEXO	REQUISITO ISO 27001	Seleccionado (S/N)	Razón para la selección / Justificación para su exclusión
15.1.3	PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN	SI	Requisito legal del modelo estándar de control interno MECI1000 (Subsistema de gestión de información) y el subsistema de gestión de la calidad de IPES
15.1.4	PROTECCIÓN DE LOS DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL	SI	Requerimiento de la ley 1581 de 2012, protección de datos personales
15.1.5	PREVENCIÓN DEL USO INADECUADO DE LOS SERVICIO DE PROCESAMIENTO DE INFORMACIÓN	SI	Requisito legal del modelo estándar de control interno MECI1000 (Subsistema de gestión de información) y el subsistema de gestión de la calidad de IPES
15.1.6	REGLAMENTACIÓN DE LOS CONTROLES CRIPTOGRÁFICOS	SI	Control seleccionado para proteger la información clasificada como reservada o sensible personal que es transmitida a terceros
15.2	CUMPLIMIENTO DE LAS POLÍTICAS Y LAS NORMAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO		
15.2.1	CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	SI	Requisitos de control interno del Modelo Estándar de Control Interno
15.2.2	VERIFICACIÓN DEL CUMPLIMIENTO TÉCNICO	SI	Requisitos de control interno del Modelo Estándar de Control Interno
15.3	CONSIDERACIÓN DE LA AUDITORIA DE LOS SISTEMAS DE INFORMACIÓN		
15.3.1	CONTROLES DE AUDITORIA DE LOS SISTEMAS DE INFORMACIÓN	SI	Requisitos de control interno del Modelo Estándar de Control Interno
15.3.2	PROTECCIÓN DE LAS HERRAMIENTAS DE AUDITORIA DE LOS SISTEMAS DE INFORMACIÓN	SI	Requisitos de control interno del Modelo Estándar de Control Interno
		10	

16 CONTROL DE CAMBIOS AL DOCUMENTO:

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO