MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

SuperSubsidio
Vigilamos tu caja de compensación

Oficina de Tecnologías de la Información y las Comunicaciones

Calle 45 A # 9-46
Teléfonos: 3487777 - PBX: 3487800
Fax 3487804
www.ssf.gov.co - e-mail: ssf@ssf.gov.co
Bogotá D.C., Colombia

SuperSubsidio Vigilamos tu caja de compensación	**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	CODIGO: MAN-GSI-XXX
		VERSION: 1
	Manual de Políticas de Seguridad de la Información	FECHA: 29/Sep./2015

Contenido

INTRODUCCIÓN

Para llevar a cabo la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) como elemento integral en todos los procesos de la SSF, es necesario difundir las Políticas de Seguridad de la Información entre todos los funcionarios, contratistas y demás colaboradores de la entidad. El mecanismo para darle un carácter de obligatoriedad al cumplimiento de estas políticas de seguridad de la información es la creación de un Manual de Políticas de Seguridad de la Información. A partir de la creación y divulgación de este manual entre todos los colaboradores de la entidad, se podrá proceder a realizar planes de sensibilización permanentes que conlleven a la apropiación de estas Políticas como parte integral de sus funciones laborales.

Este manual es desarrollado con base a las cláusulas de la norma ISO 27001:2013, el Marco de Referencia de Arquitectura Empresarial de MinTIC, el Modelo de Seguridad y Privacidad de la Información v 3.0 de MinTIC y los lineamientos de Gobierno en Línea (GEL).

El presente Manual de Políticas de Seguridad de la Información, se encuentra estructurado a partir del desarrollo de las principales áreas identificadas globalmente en la Superintendencia del Subsidio Familiar, donde se encuentran: Políticas concernientes a la Administración, Políticas concernientes a la Oficina de TIC y Políticas concernientes a Infraestructura (servicios administrativos). Cada una de las Políticas está estructurada de tal forma que presenta un título de la Política y una definición de la Política.

1. PRESENTACIÓN DEL MANUAL

1.1. Objetivo de Manual

El presente Manual, tiene por objeto integrar todas las políticas de seguridad de la información que deben ser incorporadas a la Superintendencia de Subsidio Familiar, con el fin de que al publicarse a todos los funcionarios y demás colaboradores de la entidad este manual de políticas, se convierta en la herramienta o canal de apropiación del Sistema de Gestión de Seguridad de la

Información para cada funcionario o colaborador de la entidad a través de un proceso continuo de divulgación y concientización.

1.2. Alcance de las Políticas de Seguridad de la Información

El presente Manual de Políticas de Seguridad de la Información es parte integral de todos los procesos de la Superintendencia de Subsidio Familiar y es de obligatorio cumplimiento por parte de todos los funcionarios y demás colaboradores de la entidad.

2. TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN

Los siguientes términos y definiciones están basados en el estándar NTC ISO/IEC 27001: 2013 y son aplicables a la Superintendencia del Subsidio Familiar y al PGSI de la misma:

Aceptación de riesgo: Decisión de asumir un riesgo.

Activo: cualquier elemento que represente valor para la organización.

Alta Dirección: Se considera Alta Dirección a los directivos con cargo más alto en una organización; el Presidente, el Gerente General y los Directores de las distintas áreas. En el caso de la Superintendencia del Subsidio Familiar se entiende como Alta Dirección a la integrada por la Superintendente y el Comité Directivo.

Análisis de Riesgo: Uso sistemático de la información para identificar fuentes y para estimar el riesgo (Guía ISO/IEC 73:2002).

Adaptabilidad: Define que todos los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes designados por la Alta Dirección con el objetivo de garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

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

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad

Dueño del riesgo sobre el activo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Información: Datos que poseen una información.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad d la información.

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

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Política: actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos.

Procedimiento: Forma especificada de llevar a cabo una actividad o un proceso

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Recursos informáticos: Todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimización del trabajo con computadores y periféricos, tanto a nivel Individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de los mismos.

Registro: Documento que presenta resultados obtenidos o proporcionar evidencia de actividades desempeñadas.

Responsable de Seguridad TIC: En LA ENTIDAD el comité de seguridad de la información será el grupo encargado de realizar el seguimiento y monitoreo al Sistema de Gestión de la Seguridad de la información (SGSI).

Responsables del Activo: Personas responsables del activo de información en el proceso.

Riesgo: El efecto de la incertidumbre sobre los objetivos". (Icontec, 2011, Pág.4)

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad. [NTC-ISO/IEC 27002:2013].

Sistema de gestión de la seguridad de la información SGSI: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales que se realicen en la entidad.

Tecnología de la Información: Se refiere al hardware y software operado por el organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

3. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

3.1. Aspectos a tener en cuenta

Creación de políticas

Las políticas de la Superintendencia del Subsidio Familiar deben ser creadas por la Alta Dirección de la organización con la asesoría de las áreas técnicas responsables de los temas asociados a las mismas.

Aprobación de Políticas

Las políticas de la Superintendencia del Subsidio Familiar deben ser aprobadas por la Alta Dirección con base en las recomendaciones del Comité de Seguridad de la Información.

Actualización de políticas

Cualquier requerimiento de modificación de las políticas debe ser dirigido al Comité de Seguridad de la Información quien será el encargado de mantener actualizado el modelo de seguridad de la Superintendencia del Subsidio Familiar.

Toda modificación a las políticas debe ser aprobada por la Alta Dirección de la Entidad.

Nombre de las políticas

Siempre se hará referencia a las políticas de seguridad de la Información y a la referencia del Anexo de la NTC ISO/IEC 27001:2013 al que hace referencia cada una.

Estructura de la política

La estructura de la Política de Seguridad es:

- Título de la Política.
- Definición de la Política.

3.2. Políticas concernientes a la Administración de la Superintendencia del Subsidio Familiar (PA)

Las siguientes Políticas de Seguridad de la Información son de responsabilidad de la Administración de la Superintendencia del Subsidio Familiar según lo establecido en la NTC ISO/IEC 27001:2013.

3.2.1. Políticas de Seguridad de la Información.

3.2.1.1. PA001. Título de la Política: Política de la seguridad de la información - Ref.: ISO/IEC 27001 CL A.5.1.1

Definición de la Política: La política de Seguridad de la Información de la Superintendencia del Subsidio Familiar propende por el aseguramiento de la confidencialidad, integridad y disponibilidad de la información de la entidad, así como de los activos de la Oficina de TIC apoyada en la metodología de gestión de riesgos de la Superintendencia del Subsidio Familiar, los requerimientos regulatorios y aplicación de los estándares Internacionales, acordes con la misión de la entidad; fundamentada en el compromiso de la Alta Dirección y todos los responsables de los procesos de la entidad.

3.2.1.2. PA002. Título de la Política: Revisión de las políticas para la seguridad de la información - Ref.: ISO/IEC 27001 CL A.5.1.2

Definición de la Política: Las políticas de seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas, siendo responsabilidad de la Alta Dirección el aprobar los ajustes y cambios pertinentes. Igualmente, se deberá

actualizar las políticas de Seguridad de la Información con la frecuencia definida o cuando haya lugar a un ajuste significativo.

3.2.2. Organización de la Seguridad de la Información - Ref.: ISO/IEC 27001 CL A.6.

Con la finalidad de realizar la correcta distribución de roles y responsabilidades, atendiendo a la debida segregación de funciones, se establecen las responsabilidades para las áreas funcionales dentro de la entidad.

3.2.2.1. PA003. Título de la Política: Organización interna de la seguridad de la información - Ref.: ISO/IEC 27001 CL. A.6.1

Definición de la Política: La estructura de seguridad de la información debe estar conformada por los siguientes actores a quienes se les debe definir roles y responsabilidades, según la - Ref.: ISO/IEC 27001 CL. A.6.1.1:

- Comité de seguridad de la Información: El Comité debe administrar las iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en la entidad, así como la formulación y mantenimiento de una política de seguridad de la información para la Superintendencia del Subsidio Familiar.
- Oficial de seguridad de la información: Será el responsable por la implementación, operación, mantenimiento y mejoramiento de manera transversal en la entidad del Sistema de Gestión de Seguridad de la Información.

3.2.2.2. PA004. Título de la Política: Contacto con las autoridades - Ref.: ISO/IEC 27001 CL A.6.1.3

Definición de la Política: La entidad debe mantener contacto con las entidades que representen autoridad en temas de seguridad de la información. Lo que plantea los siguientes aspectos:

- Identificar entidades que representen autoridad en temas de seguridad de la información.
- Definir las nuevas normas y requerimientos que las autoridades establecen en el tema de seguridad de la información.

- Evaluar la forma de articular los requerimientos existentes de las entidades y/o autoridades al Sistema de Gestión de la Seguridad de la Información de la Superintendencia del Subsidio Familiar.
- Adoptar los requerimientos existentes previa aprobación del comité designado para tal fin.

3.2.2.3. PA005. Título de la Política: Gestión de grupos de interés especial - Ref.: ISO/IEC 27001 CL A.6.1.4

Definición de la Política:

Se debe mantener los contactos apropiados con grupos de interés especiales, otros foros especializados y asociaciones de profesionales en seguridad de la información. Po tal motivo, se debe identificar los grupos de interés especiales de profesionales en seguridad de la información, establecer protocolos de comunicación y responsables para la interacción entre los grupos de interés.

3.2.2.4. PA006. Título de la Política: Política de teletrabajo - Ref.: ISO/IEC 27001 CL A.6.2.2

Definición de la Política:

Con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información en un entorno de teletrabajo, se establece que la entidad debe proveer a los teletrabajadores los recursos necesarios para realizar su labor en el sitio en que la desarrollen de acuerdo a lo establecido en el decreto 0884 de 2012 y a la demás normatividad aplicable y vigente. A parte de ello se debe definir el modelo de Teletrabajo a aplicar en la SSF, identificar los funcionarios que van a contar con un esquema de teletrabajo, establecer el protocolo de asignación de recursos para trabajar en el lugar establecido y definir protocolos de monitoreo de actividades de los teletrabajadores que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

3.2.3. Seguridad de los Recursos Humanos- Ref.: ISO/IEC 27001 CL. A.7

Es de vital importancia concienciar a los funcionarios de la Superintendencia del Subsidio Familiar sobre la necesidad de generar las condiciones propicias para garantizar la confidencialidad, integridad y disponibilidad de la información, por tal razón se tienen en cuenta los siguientes requisitos para establecer controles efectivos para su realización.

3.2.3.1. PA007. Título de la Política: Proceso de Selección – Ref.: ISO/IEC 27001:2013 CL. A.7.1.1

Definición de la Política:

El Grupo de Gestión del Talento Humano de Superintendencia del Subsidio Familiar debe hacerse responsable del cumplimiento de las funciones designadas, con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información desde el proceso de preselección hasta el retiro de los funcionarios.

3.2.3.2. PA008. Título de la Política: Toma de conciencia, educación y formación en la seguridad de la información - Ref.: ISO/IEC 27001 CL. A.7.2.2.

Definición de la Política:

La Superintendencia del Subsidio Familiar debe estar comprometida en adoptar una cultura de seguridad de la información, estableciendo y manteniendo un programa anual de concienciación y capacitación para todos los funcionarios de la entidad, así como para los contratistas y terceros que tengan acceso a la información institucional y desarrollen actividades de manera permanente en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta.

Todos los funcionarios, contratistas y demás terceros al servicio de las entidades y dependencias que conforman la entidad, deben ser informados y/o capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas, por medio de procesos de sensibilización y/o guías especificas del SGSI.

3.2.3.3. PA009. Título de la Política: Proceso disciplinario Ref.: ISO/IEC 27001:2013 CL. A.7.2.3

Definición de la Política:

La actuación intencionada de cualquier funcionario de la entidad donde se comprometa la confidencialidad, integridad y disponibilidad de la información debe ser sancionada bajo las normas administrativas y jurídicas aplicables, estipuladas

por la entidad y/o por las autoridades competentes. Para tal efecto se deberá tener en cuenta los siguientes aspectos:

- Identificar la violación incurrida a las políticas de seguridad de la información.
- Toda violación a las políticas de licenciamiento de software, será motivo de sanciones aplicables al personal que incurra en esta.
- Cualquier violación a la seguridad por parte del personal que labora en la entidad, así como terceros que tengan relación o algún tipo de contrato con la Superintendencia del Subsidio Familiar, se harán acreedores de sanciones aplicables acorde a la normatividad vigente.

3.2.3.4. PA010. Título de la Política: Terminación de contrato o cambio de responsabilidad en el empleo – Ref.: ISO/IEC 27001 CL A.7.3.1.

Definición de la Política:

En el momento de la desvinculación o de cambio de roles o responsabilidades de algún funcionario, contratista y/o tercero de la entidad, se debe hacer entrega de todos los activos de información que le hayan sido asignados mediante el formato establecido.

El Grupo de Gestión de Talento Humano debe notificar a la Oficina de TIC de la desvinculación, cambio de rol o responsabilidad de los funcionarios, para que ésta retire o cambie los derechos (privilegios) de acceso a la información de esos funcionarios.

3.2.4. Gestión de los activos de información- Ref.: ISO/IEC 27001 CL A.8.

Dentro de las responsabilidades de la Superintendencia del Subsidio Familiar se encuentra la custodia sobre todo tipo de información generada por la entidad misma o sus dependientes y que genere un impacto dentro de la entidad, así mismo se monitorea el almacenamiento de documentos o archivos.

3.2.4.1. PA011. Título de la Política: Clasificación de la información - Ref.: ISO/IEC 27001 CL. A.8.2.1

Definición de la Política:

La información debe ser clasificada por la Superintendencia del Subsidio Familiar, en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Toda la información debe ser identificada, clasificada y documentada por los propietarios de los activos de información, siendo ellos los responsables de establecer y clasificar los mismos, dentro de las siguientes categorías:

- Reservado: Información cuya divulgación no autorizada puede ser perjudicial para los intereses o prestigio de la entidad.
- Confidencial: Información que por su contenido solo interesa a quienes va dirigido y cuya divulgación no autorizada puede ocasionar perjuicios a determinada área de la entidad o persona.
- Restringido: es aquella información dirigida a los miembros de la institución y que se debe proteger del conocimiento de personas extrañas a la misma.
- Pública: Todo documento, registro, archivo o cualquier dato que se recopile, procese o posean los usuarios no sensibles que pueda ser publicada en la página web de la Superintendencia del Subsidio Familiar.

3.2.5. Relaciones con los proveedores - Ref.: ISO/IEC 27001 CL. A.15

Los proveedores garantizan la confidencialidad e integridad de la información a la cual tengan acceso durante la permanencia en las instalaciones de la entidad.

3.2.5.1. PA012. Título de la Política: Seguridad de la información para las relaciones con proveedores - Ref.: ISO/IEC 27001 CL. A.15.1.1

Definición de la Política:

Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar, para asegurar la protección de los activos de la Superintendencia del Subsidio Familiar que sean accesibles a los proveedores:

- Los proveedores o contratistas que tengan relaciones comerciales con la entidad, se les incluirá dentro de su contrato una cláusula de confidencialidad de información.

- Los proveedores tendrán acceso limitado a información sensible de la entidad. Si para fines de su labor fuera necesario tener acceso a dicha información, está se proporcionará con ciertas medidas de seguridad, con el fin de que no pueda ser modificada o alterada por el proveedor.
- Los contratistas no podrán tener acceso a áreas o zonas donde se encuentre información sensible en la entidad. Sí fuera necesario su ingreso a determinadas áreas, será necesaria la autorización de un funcionario de la entidad, el cual debe acompañar al contratista durante el tiempo que este permanezca en dicha área.
- Los proveedores se deben anunciar en la recepción de la Superintendencia del Subsidio Familiar a su ingreso y salida, así como los equipos necesarios para la realización de su labor en la entidad.

3.2.5.2. PA013. Título de la Política: Tratamiento de la seguridad dentro de los acuerdos con proveedores - Ref.: ISO/IEC 27001 CL. A.15.1.2

Definición de la Política:

Se deben establecer y acordar todos los requisitos de seguridad de la información pertinente con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de la Oficina de TIC para la información de la entidad, teniendo en cuenta los requisitos establecidos en los acuerdos de confidencialidad pactados con el proveedor.

3.2.5.3. PA014. Título de la Política: Cadena de suministro de tecnología de información y comunicación.- Ref.: ISO/IEC 27001 CL. A.15.1.3

Definición de la Política:

Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación de la Oficina de TIC de la entidad.

3.2.5.4. PA015. Título de la Política: Seguimiento y revisión de los servicios de los proveedores. Ref.: ISO/IEC 27001 CL. A.15.2.1

Definición de la Política:

La entidad debe realizar revisiones y auditorías periódicas sobre responsabilidades convenidas en el contrato entre el contratista y la entidad, teniendo en cuenta las obligaciones contractuales establecidas.

3.2.5.5. PA016. Título de la Política: Gestión de cambios en los servicios de los proveedores - Ref.: ISO/IEC 27001 CL. A.15.2.2

Definición de la Política:

Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información , sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos, teniendo en cuenta que la Superintendencia del Subsidio Familiar es quien autoriza los cambios o modificaciones de los servicios prestados por sus proveedores.

3.2.6. Cumplimiento - Ref.: ISO/IEC 27001 CL. A.18

3.2.6.1. PA017. Título de la Política: Identificación de la legislación aplicable y de los requisitos contractuales - Ref.: ISO/IEC 27001 CL. A.18.1.1

Definición de la Política:

La entidad debe atender a todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como los requerimientos para cumplirlos. De igual manera se deben identificar y documentar explícitamente los requisitos de la legislación aplicable, y mantenerlos actualizados para el Sistema de Gestión de Seguridad de la Información de la Superintendencia del Subsidio Familiar.

- La entidad debe atender a la siguiente normativa:
    - Norma ISO/IEC 27001:2013: Establece las directrices del Sistema de Gestión de la seguridad de la información. Adicionalmente establece el rol y responsabilidad de los funcionarios y grupos de interés de la entidad y así mismo establece la metodología de identificación de los activos de información, la valoración de los riesgos, la calificación de los controles, el plan de tratamiento para la mitigación de los riesgos asociados a los activos de información, las revisiones y auditorias que se le hacen al SGSI.

- Gobierno en línea: La Superintendencia del Subsidio Familiar por ser una entidad estatal, está sujeta a la normativa aplicable para las empresas públicas en Colombia, por tal razón el Sistema de Gestión de la seguridad de la información de la entidad se ajusta a los requerimientos que por parte de gobierno en Línea se establecen para la estructuración del SGSI de la entidad.

- Los requisitos legales y regulatorios que afectan la seguridad de la información debe ser reconocidos por:
  - La Alta Dirección.
  - Los dueños de cada proceso de la entidad.
  - El Oficial de seguridad de la información.
  - Los representantes de otras áreas relacionadas con la seguridad.

Adicionalmente, de manera continua se deben realizar:

- Revisiones permanentes sobre la expedición de nuevas leyes y normatividades que afectan de manera directa la Seguridad de la Información de la entidad.
- La interpretación de las implicaciones en la seguridad de la información de estas leyes y reglamentos.
- La identificación de la posibilidad de incumplimiento legal y reglamentario por parte de la entidad.
- La determinación de acciones sobre el posible incumplimiento.

3.2.6.2. PA018. Título de la Política: Derechos de la propiedad intelectual - Ref.: ISO/IEC 27001 CL. A.18.1.1.

Definición de la Política:

La Superintendencia del Subsidio Familiar debe implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el registro de derechos de uso.

En la entidad, la política de licenciamiento de software y derechos de propiedad intelectual debe establecer que:

- La entidad debe cumplir con la reglamentación de propiedad intelectual para lo cual implementa los controles necesarios que garanticen el respeto de dicha reglamentación.
- No se permite el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.
- Se permite el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.
- Definición de normas y procedimientos para el cumplimiento de la normatividad vigente.
- Divulgación de las políticas de adquisición de software y las disposiciones de la normatividad vigente.
- Se debe mantener un adecuado registro de activos.
- Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
- Implementar controles para evitar el exceso del número máximo permitido de usuarios.
- Verificar que sólo se instalen productos con licencia y software autorizado.
- Elaboración y divulgación de un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
- Utilización de herramientas de auditoría adecuadas.
- Cumplimiento con los términos y condiciones establecidos para obtener software e información en redes públicas.
- La Oficina de TIC debe realizar un inventario de licencias de software mínimo dos veces al año, en particular de herramientas de oficina y productividad, licencia de usuario de sistemas operativos de red, base de datos y otros.
- Se debe tener control sobre el uso de software libre que hacen los usuarios, y su relación con la función que realizan.
- La Oficina de TIC debe hacer seguimiento y control sobre el uso de licencias asignadas a los usuarios, mediante una auditoria según el perfil de usuario de software establecido.

3.2.6.3. PA019. Título de la Política: Protección de registros - Ref.: ISO/IEC 27001 CL. A.18.1.2

Definición de la Política:

Los registros críticos de la entidad se deben proteger contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la entidad.

3.2.6.4. PA020. Título de la Política: Privacidad y protección de información de datos personales - Ref.: ISO/IEC 27001 CL. A.18.1.3

Definición de la Política:

La Superintendencia del Subsidio Familiar debe redactar un “Compromiso de Confidencialidad”, el cual sea suscrito por todos los funcionarios. La copia firmada del compromiso será retenida en forma segura por la entidad. Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la ley 1581de 2012, el decreto 1377 de 2013 y la demás normatividad aplicable.

Además de lo anterior la entidad debe establecer que:

- La entidad asegura la debida reserva de la información personal de las personas o empresas que se encuentran en su base de datos, la cual será utilizada para el envío de información institucional de la entidad.
- La entidad no proporciona la información de sus grupos de interés a ningún tercero, salvo que la persona o empresa lo autorice de forma expresa y por escrito.
- Las empresas o personas pueden decidir, conocer, actualizar, rectificar y solicitar la eliminación de sus datos personales en cualquier momento a la entidad.
- La información obtenida en cualquier evento en que participe en la entidad, será utilizada solo para fines institucionales, en ningún momento será compartida ni transferida a terceros para su utilización.

3.2.6.5. PA021. Título de la Política: Revisión independiente de la seguridad de la información - Ref.: ISO/IEC 27001 CL. A.18.2.1

Definición de la Política:

La Auditoría Interna, Control Interno o en su defecto quien sea designado por el Comité de Seguridad de la Información debe realizar revisiones independientes sobre la vigencia e implementación de las Políticas de Seguridad de la

Información, a efectos de garantizar que las prácticas de la Superintendencia del Subsidio Familiar reflejan adecuadamente sus disposiciones, teniendo en cuenta los siguientes parámetros:

- Garantizar la pertinencia de las políticas y lineamientos establecidos para la entidad.
- Evaluar la eficacia, eficiencia y efectividad del SGSI.
- Determinar si existen nuevos requerimientos o actualizaciones de la norma.
- Establecer los cambios y modificaciones que sean necesarias al SGSI.
- Someter a discusión en el comité designado en la entidad los cambios a realizar.
- Aprobar y dejar documentado las modificaciones realizadas al SGSI.

3.2.6.6. PA022. Título de la Política: Revisión y cumplimiento de las políticas y normas de seguridad - Ref.: ISO/IEC 27001 CL. A.18.2.2 y A.18.2.3

Definición de la Política:

El oficial de seguridad debe velar por el cumplimiento del procesamiento y procedimientos de gestión de la información dentro de la Superintendencia del Subsidio Familiar, con las políticas y normas de seguridad apropiadas. Así mismo los funcionarios deben dar cumplimiento a las políticas y normas de seguridad.

En caso de ser identificado algún tipo de incumplimiento de las políticas o normas de seguridad, el Oficial de Seguridad debe realizar lo siguiente:

- Establecer las causas del incumplimiento.
- Evaluar las acciones correctivas adecuadas para tratar las causas que generan el incumplimiento.
- Determinar la acción correctiva escogida.
- Revisar y hacer seguimiento al plan de tratamiento o acción de mejora emprendida.

3.3. Políticas concernientes a la Oficina TIC de la Superintendencia del Subsidio Familiar (PTI)

Las siguientes Políticas de Seguridad de la Información son responsabilidad de la Oficina de TIC de la entidad según la NTC ISO 27001:2013.

3.3.1. Políticas de Seguridad de la Información - Ref.: ISO/IEC 27001 CL. A.5.

3.3.1.1. PTI001. Título de la Política: Políticas para la administración del riesgo en la seguridad de la información- - Ref.: ISO/IEC 27001 CL. A.5.1.

Definición de la Política:

Los dueños de cada proceso en la Oficina de TIC de la Superintendencia del Subsidio Familiar deben identificar, analizar y evaluar los riesgos asociados a sus activos de información, al mismo tiempo que implementan acciones tanto correctivas como preventivas establecidas en el plan de tratamiento del SGSI. De igual manera los funcionarios de la entidad tienen conocimiento de los riesgos, causas y vulnerabilidades de cada activo de información, con el fin de gestionar el riesgo de manera oportuna, garantizando así los principios de confidencialidad, integridad y disponibilidad de la información.

3.3.1.2. PTI002. Título de la Política: Política para los dispositivos móviles - Ref.: ISO/IEC 27001 CL A.6.2.1

Definición de la Política:

Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, la Oficina de TIC debe implementar controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

3.3.2. Gestión de los activos de información- Ref.: ISO/IEC 27001 CL A.8

Dentro de las responsabilidades de la Superintendencia del Subsidio Familiar se encuentra la custodia sobre todo tipo de información generada por la entidad misma o sus dependientes y que genere un impacto dentro de la entidad, así mismo se monitorea el almacenamiento de documentos o archivos.

3.3.2.1. PTI003. Título de la Política: Inventario de activos - Ref.: ISO/IEC 27001 CL A.8.1.1

Definición de la Política:

La Superintendencia del Subsidio Familiar debe identificar los activos asociados con la información e instalaciones de procesamiento de información, y debe elaborar y mantener un inventario de estos activos.

Todos los activos de información de software, hardware, servicios, bases de datos o cualquier otro que sea diseñado o desarrollado para la entidad, de manera directa o indirecta con ocasión de convenios o contratos con organismos públicos, gubernamentales o entidades particulares o privadas, son de propiedad de la Superintendencia del Subsidio Familiar y hacen parte del inventario de activos de la entidad.

3.3.2.2. PTI004. Título de la Política: Propiedad de los activos - Ref.: ISO/IEC 27001 CL A.8.1.2

Definición de la Política:

Los activos de información deben tener un propietario o responsable asociado, quien velará por su buen uso y custodia. Quien se encargará de hacer la evaluación de criticidad, de definir el nivel de clasificación y ser quien define los requisitos de seguridad del activo.

3.3.2.3. PTI005. Título de la Política: Uso aceptable de los activos - Ref.: ISO/IEC 27001 CL A.8.1.3

Definición de la Política:

Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información, así como las instalaciones de procesamiento de la misma. Los funcionarios de la entidad deben hacer buen uso de los activos de información designados para su labor dentro de la entidad conforme a la ley 734 de 2002 y la demás normatividad vigente.

3.3.2.4. PTI006. Título de la Política: Devolución de activos - Ref.: ISO/IEC 27001 CL A.8.1.4

Definición de la Política:

Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

3.3.2.5. PTI007. Título de la Política: Gestión de medios removibles - Ref.: ISO/IEC 27001 CL. A.8.3.1

Definición de la Política:

Se debe restringir la conexión no autorizada de cualquier elemento de almacenamiento externo, como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales o no autorizados por la entidad.

Los medios de almacenamiento removibles como cintas, discos duros removibles, CDs, DVDs, medios impresos y dispositivos USB, entre otros, que contengan información institucional, deben ser controlados y físicamente protegidos.

3.3.3. Control de accesos- Ref.: ISO/IEC 27001 CL. A.9

Para la entidad debe ser prioritario definir el personal que tenga acceso a información sensible, por lo cual ha limitado el acceso de usuarios de aplicaciones computarizadas únicamente a los funcionarios y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la información puede ser sensible o tener un carácter confidencial. Así mismo es necesario restringir el acceso a las instalaciones donde dicha información se encuentra guardada, garantizando así la confidencialidad e integridad de la misma.

3.3.3.1. PTI008. Título de la Política: Política de control y Administración de accesos - Ref.: ISO/IEC 27001 CL. A.9.1.1

Definición de la Política:

La Superintendencia del Subsidio Familiar debe establecer que los funcionarios, contratistas, pasantes y demás personal que tenga acceso a la información de la entidad:

- Son usuarios de la red de la entidad todos los empleados, trabajadores oficiales, los trabajadores en misión, los contratistas, los pasantes y terceros, bien sea personas naturales o empresas que estén de forma temporal o permanente en la Superintendencia del Subsidio Familiar.

- El acceso a la red por parte de terceros debe estar estrictamente restrictivo y permisible únicamente mediante firma impresa y documentación de aceptación de la confidencialidad hacia la entidad y comprometido con el uso exclusivo del servicio para el que fue provisto el acceso.

3.3.3.2. PTI009. Título de la Política: Seguridad para Internet.- - Ref.: ISO/IEC 27001 CL. A.9.1.2

Definición de la Política:

El acceso a Internet debe ser utilizado con propósitos autorizados o con el destino por el cual fue provisto. La Oficina de TIC debe definir los procedimientos para solicitar y aprobar accesos a Internet. Los accesos son autorizados formalmente por el Responsable de la Unidad Organizativa a cargo del personal que lo solicite. Asimismo, se definen las pautas de utilización de Internet para todos los usuarios.

3.3.3.3. PTI010. Título de la Política: Seguridad para redes inalámbricas.- - Ref.: ISO/IEC 27001 CL. A.9.1.2

Definición de la Política:

Para tener acceso a cualquier red inalámbrica, los funcionarios, contratistas y demás personas que se conecten a las redes inalámbricas de la entidad deben:

- Conectarse a las redes inalámbricas en la red de la entidad a través de protocolos seguros (Radius).
- Acceder a la red inalámbrica de la entidad los usuarios y equipos autorizados mediante la asociación de las direcciones MAC de los portátiles a las direcciones IP asignadas.

3.3.3.4. PTI011. Título de la Política: Administración de cuentas - Ref.: ISO/IEC 27001 CL. A.9.2.1

Definición de la Política:

En la Superintendencia del Subsidio Familiar, los funcionarios, contratistas, pasantes, empleados en misión o cualquier persona deben pasar por un proceso formal de registro y/o de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

3.3.3.5. PTI012. Título de la Política: Política de Gestión de contraseñas- Ref.: ISO/IEC 27001 CL. A.9.4.3

Definición de la Política:

El sistema de control de contraseñas debe asegurar la calidad de las mismas, teniendo en cuenta una parametrización basada en buenas prácticas y el nivel de criticidad de cada Sistema de Información. Se debe aplicar, divulgar y monitorear el cumplimiento de la política de contraseñas (basado en buenas prácticas), mediante la definición y ejecución de procesos, procedimientos y guías pertinentes.

3.3.4. Criptografía - Ref.: ISO/IEC 27001 CL. A. 10

Con el fin de garantizar la confidencialidad e integridad de algunos documentos designados como sensibles, la entidad utilizará sistemas y técnicas criptográficas para la protección de la información.

3.3.4.1. PTI013. Título de la Política: Política sobre el uso de controles criptográficos (Protección de la Información) - Ref.: ISO/IEC 27001 CL. A. 10.1.1

Definición de la Política:

El sistema de información debe implementar mecanismos de protección de información que cumplan con la reglamentación, políticas, estándares, guías aplicables, así como:

- Proporcionar una protección adecuada a los equipos utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
- Proteger las claves secretas y privadas evitando sean copiadas o modificadas sin autorización.

3.3.4.2. PTI014. Título de la Política Gestión de llaves - Ref.: ISO/IEC 27001 CL. A. 10.1.2

Definición de la Política:

Se debe implementar en la entidad un sistema de administración de claves criptográficas para garantizar la confidencialidad e integridad de la información sensible de la entidad, para lo cual, las claves criptográficas se convierten en un

activo de información esencial para proteger la confidencialidad e integridad de la información, garantizando así que tanto el emisor como el receptor de la información, envían y reciben información fidedigna, verás e integra.

3.3.5. Seguridad de las operaciones - Ref.: ISO/IEC 27001 CL. A. 12

Se protege la seguridad de las operaciones en las instalaciones de procesamiento de la información, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

3.3.5.1. PTI015. Título de la Política: Operaciones documentadas - Ref.: ISO/IEC 27001 CL. A. 12.1.1

Definición de la Política:

Se debe documentar y mantener actualizados todos los procedimientos de operación, teniendo en cuenta los ya existentes en la entidad, asegurando la disponibilidad de la información.

3.3.5.2. PTI016. Título de la Política: Gestión de cambios - Ref.: ISO/IEC 27001 CL. A. 12.1.2

Definición de la Política:

Se debe mantener un control de los cambios en la entidad, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información y se debe justificar la razón de dichos cambios, los cuales serán revisados y evaluados por parte de la Oficina de TIC, el Oficial de seguridad y las partes interesadas en la entidad.

3.3.5.3. PTI017. Título de la Política: Gestión de capacidad - Ref.: ISO/IEC 27001 CL. A. 12.1.3

Definición de la Política:

La Oficina de TIC o la persona que sea designada por el área realizará una revisión periódica sobre las necesidades de capacidad de las instalaciones y de los sistemas de procesamiento de la información, debiéndose proyectar las

necesidades futuras de capacidad adicional, a fin de garantizar un procesamiento y almacenamiento adecuado y suficiente.

Por lo anterior se deben evaluar las necesidades actuales de almacenamiento de información y hacer una proyección de los requerimientos de capacidad en el futuro con el fin de que se generen acciones preventivas, donde se pueda gestionar el riesgo asociado a la falta o disminución capacidad de almacenamiento de información, comprometiendo la disponibilidad de la misma. Además se deben tener en cuenta las siguientes medidas:

- Implementación de los mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma sean periódicamente monitoreados, afinados y proyectados para futuros requerimientos de capacidad de procesamiento y comunicación.
- El responsable de cada componente de la plataforma tecnológica debe realizar el monitoreo permanente sobre éste.

3.3.5.4. PTI018. Título de la Política: Separación de los ambientes de desarrollo, de pruebas y operación. - Ref.: ISO/IEC 27001 CL. A. 12.1.4

Definición de la Política:

Se deben establecer roles y responsabilidades en cada fase del desarrollo o modificación de los sistemas de información de la entidad y a su vez se deben separar los ambientes de desarrollo, pruebas y producción, con el fin de garantizar la integridad y disponibilidad de la información.

Se deben proveer los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y/o física entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación. Por lo anterior se deben tomar en consideración los siguientes factores:

- El paso de software y hardware de un ambiente a otro se controla y gestiona.
- Los usuarios cuentan únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.

ISO 9001 icontec
NTCGP 1000 icontec
IQNet

- No se realizan pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información.
- El ambiente del sistema de prueba emula el ambiente de producción lo más estrechamente posible.
- No se permite la copia de información Reservada, Confidencial, Restringida o Exclusiva de la entidad, desde el ambiente de producción al ambiente de pruebas; en caso de que sea estrictamente necesario, la copia la autoriza el propietario de la información y el Oficial de Seguridad de la Información y se implementan controles que garanticen que la confidencialidad de la información sea protegida y se elimine de forma segura después de su uso.
- Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.
- Periódicamente se verifican las versiones instaladas tanto en ambiente de pruebas como en producción y confrontan esta información con revisiones previas y con las versiones de programas fuentes almacenadas en los repositorios de la cada dependencia y entidad del sector.
- Se establecen roles y responsabilidades en cada fase del desarrollo o modificación de los sistemas de información de la entidad y a su vez se separan los ambientes de desarrollo, pruebas y producción, con el fin de garantizar la integridad y disponibilidad de la información.

3.3.5.5. PTI019. Título de la Política: Controles contra códigos maliciosos- Ref.: ISO/IEC 27001 CL. A. 12.2.

Definición de la Política:

Para asegurarse de que la información y las instalaciones de procesamiento de la información estén protegidos contra códigos maliciosos se deben implementar controles de detección de prevención y de recuperación, combinados con la toma de conciencia de protección de los usuarios contra códigos maliciosos.

3.3.5.6. PTI020. Título de la Política: Respaldo de la información. - Ref.: ISO/IEC 27001 CL. A. 12.3.1

Definición de la Política:

Las copias de seguridad de los sistemas de computación deben estar almacenadas en una zona diferente de donde reside la información original. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente con el fin de asegurar la integridad y disponibilidad de la información.

3.3.5.7. PTI021. Título de la Política: Registro de eventos - Ref.: ISO/IEC 27001 CL. A. 12.4.1

Definición de la Política:

Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

3.3.5.8. PTI022. Título de la Política: Protección de la información de registro - Ref.: ISO/IEC 27001 CL. A. 12.4.2

Definición de la Política:

La Oficina de TIC en conjunto con el Oficial de Seguridad de la Información, los propietarios de los riesgos asociados a los activos de información deben establecer los criterios necesarios que permiten el aseguramiento de la información, basados en el nivel de criticidad de cada activo de la entidad. Por tal razón, las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

3.3.5.9. PTI023. Título de la Política: Registros del administrador y del operador - Ref.: ISO/IEC 27001 CL. A. 12.4.3

Definición de la Política:

Para garantizar la integridad de la información debe existir un registro de cualquier modificación realizada al sistema de procesamiento de la información, por tal razón se debe tener en cuenta lo siguiente:

- Llevar un registro documentado en el que se consignen las solicitudes de modificación o de cambios que se hayan realizado a los sistemas de procesamiento de información.
- Documentar de manera clara y explícita cuando hayan ocurrido fallas, la forma como fueron corregidas y el porcentaje de avance de la acción de mejora.

3.3.5.10. PTI024. Título de la Política: Gestión de las vulnerabilidades técnicas - Ref.: ISO/IEC 27001 CL. A. 12.6.1

Definición de la Política:

Con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información en el sistema de información y procesamiento de la información se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la entidad a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

3.3.5.11. PTI025. Título de la Política: Restricciones sobre la instalación y/o actualización de software - Ref.: ISO/IEC 27001 CL. A. 12.6.2 y A. 12.5.1

Definición de la Política:

Los funcionarios de la entidad no podrán instalar ningún software, programa o aplicativo en los equipos designados para su labor en la entidad o bajo la modalidad de teletrabajo.

En el caso en que se requiera su instalación el funcionario debe pedir la autorización a su jefe inmediato, justificando de forma escrita la necesidad de la instalación del nuevo software. Cuando sea autorizado por el jefe inmediato, él le escalará el requerimiento a la Oficina de TIC siendo la única área autorizada para la instalación del nuevo software en los equipos de la entidad.

3.3.6. Seguridad de las comunicaciones - Ref.: ISO/IEC 27001 CL. A. 13

Es de vital importancia la transmisión de información desde y hacia la entidad, por tal razón se establecen ciertos parámetros que garantizan la confidencialidad e integridad de la información.

3.3.6.1. PTI026. Título de la Política: Control de redes - Ref.: ISO/IEC 27001 CL. A. 13.1.1

Definición de la Política:

El acceso a las redes de la Superintendencia del Subsidio Familiar debe estar limitado a los funcionarios de la entidad y demás personas autorizadas por la misma por medio de claves de acceso a los sistemas de información, con la finalidad de disminuir el acceso no autorizado de personal ajeno a la entidad.

3.3.6.2. PTI027. Título de la Política: Seguridad de los servicios de red - Ref.: ISO/IEC 27001 CL. A. 13.1.2

Definición de la Política:

Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

Con el fin de garantizar la confidencialidad e integridad de la información se deben establecer las siguientes medidas:

- Mantener instalados y habilitados sólo aquellos programas, aplicativos o servicios que sean utilizados por los funcionarios de la entidad o demás personas autorizadas para su manejo.
- Controlar el acceso lógico a los programas, aplicativos o servicios tanto de los usuarios como de los administradores.
- Configurar cada programa, aplicativo o servicio de manera segura, evitando las vulnerabilidades que se pudieran presentar.
- Instalar y verificar periódicamente las actualizaciones de seguridad realizadas.

3.3.6.3. PTI028. Título de la Política: Separación de redes - Ref.: ISO/IEC 27001 CL. A. 13.1.3

Definición de la Política:

La arquitectura de red de la entidad debe considerar la separación de redes de acuerdo al nivel de confidencialidad y la clase de información que se almacena en los sistemas que constituyen dichas redes.

3.3.6.4. PTI029. Título de la Política: Transferencia de la información - Ref.: ISO/IEC 27001 CL. A.13.2.

Definición de la Política:

Se debe prohibir el envío de información confidencial o sensible de la entidad a personal externo de la entidad sin autorización previa.

- Está prohibido el uso del correo electrónico personal (Hotmail, gmail...) para el envío o recepción de cualquier tipo de información relacionada con la entidad.
- Cualquier información que entre o salga de la entidad por medio magnético, transmisión electrónica o hardware, deberá tener los mecanismos de autenticación, autorización y registro de los eventos que aseguren la confidencialidad, integridad, auditabilidad y disponibilidad de esta información.

3.3.6.5. PTI030. Título de la Política: Acuerdos sobre transferencia de información - Ref.: ISO/IEC 27001 CL. A. 13.2.2

Definición de la Política:

Se debe contar con procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones, en concordancia con la normatividad vigente.

Las alianzas y convenios con los proveedores estarán regidos bajo los siguientes criterios:

- Cualquier alianza o convenio de procesamiento de información con proveedores o con personal externo a la entidad debe contar con mecanismos de confidencialidad, integridad y auditabilidad de tal forma que cumpla con los estándares definidos por seguridad de la información de la entidad.
- La información referente a servicios, tramites e información entre la entidad y los usuarios de la página web, debe tener la seguridad necesaria para el

uso de registro de usuarios, gestión de sesiones seguras, generación de registros de auditoría y validez jurídica para dar pleno valor probatorio a los mensajes de datos, de conformidad con los dispuesto por la ley 527 de 1999.

- Para todo el intercambio de información confidencial o restringida se deben establecer acuerdos de confidencialidad.

3.3.6.6. PTI031. Título de la Política: Mensajería electrónica - Ref.: ISO/IEC 27001 CL. A.13.2.3

Definición de la Política:

Con el fin de garantizar la confidencialidad de la información, se deben establecer parámetros para el envío de la información a terceros por medio del correo electrónico de la entidad para proteger adecuadamente la información incluida en la mensajería electrónica, para tal fin:

- Los funcionarios de la Superintendencia del Subsidio Familiar serán responsables de todas las actividades realizadas con su cuenta de correo institucional.
- Los empleados de la Entidad no entregarán, ni compartirán la clave del correo institucional asignado para el desarrollo de sus funciones a otros funcionarios ni a terceras personas.
- En el caso de recibir un correo electrónico de un destinatario desconocido, esté no debe ser abierto y el empleado debe notificar de forma inmediata, para evitar que en caso de que este contenga algún virus, infecte el sistema.
- El servicio de correo electrónico debe ser usado únicamente para el ejercicio de las funciones de competencia de cada usuario.
- El uso indebido del servicio de correo electrónico es motivo de suspensión temporal de su cuenta de correo o la eliminación total de la cuenta dentro del sistema.
- La entidad se reserva el derecho de monitoreo del servicio de correo electrónico el cual será realizado por el Oficial de Seguridad de la Información en conjunto con la Alta Dirección.

3.3.6.7. PTI032. Título de la Política: Acuerdos de confidencialidad o de no divulgación - Ref.: ISO/IEC 27001 CL. A.13.2.4

Definición de la Política:

Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

En todo convenio o contrato que la Superintendencia del Subsidio Familiar firme con sus funcionarios, contratistas, pasantes y demás personal será necesario:

- Establecer una cláusula de confidencialidad de la información.
- En el caso de los contratistas se les incluirá dentro de los contratos de sus empleados, cláusulas de confidencialidad y reserva de la información a la cual tengan acceso mientras permanezcan en la entidad.

3.3.7. Adquisición, desarrollo y mantenimiento de sistemas - Ref.: ISO/IEC 27001 CL. A. 14

Con la finalidad de garantizar la continuidad del negocio y la disponibilidad de la información se establecen las siguientes directrices:

3.3.7.1. PTI033. Título de la Política: Adquisición y Mantenimiento de Sistemas- Ref.: ISO/IEC 27001 CL. A.14.1

Definición de la Política:

La Superintendencia del Subsidio Familiar debe asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

3.3.7.2. PTI034. Título de la Política: Análisis y especificación de requisitos de seguridad de la información- Ref.: ISO/IEC 27001 CL. A.14.1.1

Definición de la Política:

La Superintendencia del Subsidio Familiar establecerá los requisitos relacionados con seguridad de la información, los cuales deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

3.3.7.3. PTI035. Título de la Política: Seguridad de servicios de las aplicaciones en redes públicas.- Ref.: ISO/IEC 27001 CL. A.14.1.2

Definición de la Política:

La oficina de TIC debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas la información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas.

3.3.7.4. PTI036. Título de la Política: Protección de transacciones de los servicios de las aplicaciones.- Ref.: ISO/IEC 27001 CL. A.14.1.3

Definición de la Política:

La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la trasmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada por medio de controles que establecerá la Oficina de TIC.

3.3.7.5. PTI037. Título de la Política: Desarrollo seguro - Ref.: ISO/IEC 27001 CL. A.14.2.1

Definición de la Política:

Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrolladores ya sea dentro de la organización o externos.

3.3.7.6. PTI038. Título de la Política: control de cambios en el sistema - Ref.: ISO/IEC 27001 CL. A.14.2.2

Definición de la Política:

Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios establecidos y documentados por la Oficina de TIC con la previa autorización a la ejecución de dichos cambios, evitando que se afecte la integridad, confidencialidad y disponibilidad de la Información.

Para realizar cambios tecnológicos en la Superintendencia del Subsidio Familiar es necesario tener en cuenta las siguientes consideraciones:

- Los cambios que afecten la plataforma tecnológica deben contribuir y mantener los niveles de seguridad informática y serán aprobados por la Oficina de TIC.
- Bajo ninguna circunstancia el cambio de un sistema de información o una plataforma tecnológica puede ser aprobado, desarrollado e implantado por la misma persona, se requiere de la aprobación por parte de la Oficina de TIC.
- Los cambios técnicos en los sistemas de información o en la plataforma tecnológica son documentados por la Oficina de TIC, debiéndose aprobar de acuerdo con la metodología de documentación de la entidad para ese aspecto.
- Todo cambio que se realice en los sistemas de información o en la plataforma es priorizado de acuerdo con la necesidad del requerimiento y la importancia para la operación de la entidad.
- Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deben seguir los lineamientos definidos en el Procedimiento de Control de Cambios.

3.3.7.7. PTI039. Título de la Política: Revisión técnica de las aplicaciones después de cambios en la plataforma de operación - Ref.: ISO/IEC 27001 CL. A.14.2.3

Definición de la Política:

Cuando se cambian las plataformas de operación, la Oficina de TIC debe revisar las aplicaciones críticas del negocio, y someterlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la entidad provocado por los cambios previamente aprobados ye ejecutados por la Oficina de TIC.

3.3.7.8. PTI040. Título de la Política: Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.- Ref.: ISO/IEC 27001 CL. A.14.2.3

Definición de la Política:

Los cambios a los paquetes de software son autorizados, supervisados y realizados por funcionarios por la Oficina de TIC de la entidad. Si es necesario que un proveedor o contratista realice los cambios al paquete de Software, estos cambios serán realizados bajo el permiso y supervisión de la misma área, con la

finalidad de garantizar la confidencialidad e integridad de la información contenida en los computadores, dispositivos móviles, sistemas de información y procesamiento a los que sea necesario realizarle cambios.

3.3.7.9. PTI041. Título de la Política: Restricciones en los cambios a los paquetes de software - Ref.: ISO/IEC 27001 CL. A.14.2.4

Definición de la Política:

Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente, siendo la Oficina de TIC la única autorizada para realizar cambios a los paquetes de software en la entidad con previa solicitud de los jefes de cada área que así lo requieran.

3.3.7.10. PTI042. Título de la Política: Desarrollo contratado externamente - Ref.: ISO/IEC 27001 CL. A.14.2.7

Definición de la Política:

Será responsabilidad de la Oficina de TIC de la entidad supervisar durante los ambientes de desarrollo, de pruebas, de aseguramiento de la calidad y de producción los desarrollos hechos por los contratistas.

- El nuevo software garantizará la confidencialidad, integridad y disponibilidad de los demás sistemas de información, aplicaciones, programas con los que cuente la entidad.
- La Oficina de TIC debe verificar el avance del desarrollo, acorde a las condiciones pactadas en el contrato que la entidad y el contratista hayan suscrito.

3.3.7.11. PTI043. Título de la Política: Pruebas de seguridad de sistemas - Ref.: ISO/IEC 27001 CL. A.14.2.8

Definición de la Política:

Para los Sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados por parte de la Oficina de TIC.

Con la finalidad de garantizar la disponibilidad de la información se deben realizar las siguientes pruebas:

- Pruebas de compatibilidad: Se debe garantizar el funcionamiento adecuado y continúo del software desarrollado en diferentes plataformas: hardware, sistemas operativos, redes.
- Pruebas de integración: Se debe comprobar las conexiones y comunicaciones entre los diferentes módulos del software desarrollado y los demás sistemas de información de la entidad que tengan relación con el desarrollo.
- Pruebas de función: Esta prueba permite asegurar que el sistema cumple con la funcionalidad para el cual fue hecho, con las especificaciones técnicas esperadas y es útil para los funcionarios de la entidad.
- Pruebas de desempeño: La finalidad de esta prueba está orientada a establecer la eficiencia del sistema de información cuando es utilizado por parte de los funcionarios de la entidad, estableciendo posibles fallas antes de su puesta en marcha.
- Pruebas de instalación: Esta prueba consiste en instalar el sistema de información en el servidor que alojará la base de datos o los archivos fuente del sistema de información.

3.3.8. Gestión de incidentes de seguridad de la información - Ref.: ISO/IEC 27001 CL. A.16

La entidad gestiona los incidentes de forma eficaz y eficiente, de tal forma que se disminuya el impacto que se pudiera generar en la entidad.

3.3.8.1. PTI044. Título de la Política: Responsabilidades y procedimientos - Ref.: ISO/IEC 27001 CL. A.16.1.1

Definición de la Política:

La Superintendencia del Subsidio Familiar debe establecer acciones que mitiguen el impacto asociado a los incidentes que se presentan, por tal razón se establecerán los procedimientos para la gestión de los incidentes de seguridad de la información.

Adicionalmente por requerimiento GEL “La entidad debe implementar una capacidad de manejo de incidentes, de manera que incluya: preparación, detección, análisis, contención, erradicación y recuperación”.

3.3.8.2. PTI045. Título de la Política: Reporte de eventos de seguridad de la información - Ref.: ISO/IEC 27001 CL. A.16.1.2

Definición de la Política:

Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. Todos los funcionarios, contratistas y terceros que utilizan los sistemas y servicios de información, deben notificar y reportar cualquier debilidad de seguridad observada o sospechada al oficial de seguridad o a las autoridades de seguridad de la información establecidos en la entidad.

3.3.8.3. PTI046. Título de la Política: Evaluación de eventos de seguridad de la información y decisiones sobre ellos - Ref.: ISO/IEC 27001 CL. A.16.1.4

Definición de la Política:

La entidad debe probar periódicamente (por lo menos una vez al año), la capacidad de respuesta a incidentes del sistema de información para determinar la efectividad de la respuesta al incidente y documenta los resultados.

3.3.8.4. PTI047. Título de la Política: Aprendizaje obtenido de los incidentes de seguridad de la información - Ref.: ISO/IEC 27001 CL. A.16.1.6

Definición de la Política:

Se debe tener en cuenta el tratamiento realizado para la gestión de incidentes anteriores, los cuales serán tenidos en cuenta para ser evaluados como posibles soluciones para incidentes futuros en la entidad.

3.3.8.5. PTI048. Título de la Política: Recolección de evidencia.- Ref.: ISO/IEC 27001 CL. A.16.1.7

Definición de la Política:

La Superintendencia del Subsidio Familiar debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

3.3.9. Aspectos de seguridad de la información de la gestión de continuidad del negocio - Ref.: ISO/IEC 27001 CL. A.17

La entidad implementa un proceso de continuidad de negocios con la finalidad de mitigar el impacto de acciones como desastres naturales, accidentes, fallas de los equipos y acciones deliberadas de terceros en los cuales la Superintendencia del Subsidio Familiar no tiene injerencia directa, pero establece acciones para poder recuperarse rápidamente y que la operación de la entidad no se vea comprometida.

3.3.9.1. PTI049. Título de la Política: Planificación de la continuidad de la seguridad de la información - Ref.: ISO/IEC 27001 CL. A.17.1.1

Definición de la Política:

La Superintendencia del Subsidio Familiar debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

3.3.9.2. PTI050. Título de la Política: Implementación de la continuidad de la seguridad de la información - Ref.: ISO/IEC 27001 CL. A.17.1.2

Definición de la Política:

La Superintendencia del Subsidio Familiar debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

3.3.9.3. PTI051. Título de la Política: Verificación, revisión y evaluación de la continuidad de la seguridad de la información - Ref.: ISO/IEC 27001 CL. A.17.1.3

Definición de la Política:

La Superintendencia del Subsidio Familiar debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e

implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

3.3.9.4. PTI052. Título de la Política: Disponibilidad de las instalaciones de procesamiento de información - Ref.: ISO/IEC 27001 CL. A.17.2.1

Definición de la Política:

Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad dentro de la Oficina de TIC.

3.4. Políticas concernientes a Infraestructura (Servicios Administrativos) de la Superintendencia del Subsidio Familiar (PI)

Las siguientes Políticas de Seguridad de la Información son responsabilidad del Área de Servicios Administrativos según la NTC ISO/IEC 27001:2013.

3.4.1. Seguridad física y del entorno- Ref.: ISO/IEC 27001 CL. A. 11

La seguridad física y del entorno disminuye los daños producidos por interferencias en la consulta o envío la información, adicionalmente se protege la información que se custodia o se procesa dentro de la entidad. Asimismo, permite disminuir el acceso no autorizado de personas con la intención de alterar o modificar la información.

3.4.1.1. PI001. Título de la Política: Perímetro de seguridad física - Ref.: ISO/IEC 27001 CL. A. 11.1.1

Definición de la Política:

Para evitar el acceso no autorizado a ciertos espacios considerados como sensibles dentro de la organización se deben tener perímetros de seguridad y usados para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.

3.4.1.2. PI002. Título de la Política: Controles de Accesos Físicos - Ref.: ISO/IEC 27001 CL. A. 11.1.2

Definición de la Política:

Se debe garantizar la seguridad en zonas donde se maneja información sensible de la entidad por medio de los controles de acceso físico, siendo estos definidos por el oficial de seguridad de la Superintendencia del Subsidio Familiar y la Oficina de TIC de la entidad, con la finalidad de permitir el acceso sólo al personal autorizado.

3.4.1.3. PI003. Título de la Política: Seguridad de las oficinas, recintos e instalaciones - Ref.: ISO/IEC 27001 CL. A. 11.1.3

Definición de la Política:

Para la selección y el diseño de un área protegida se deben establecer las zonas de la entidad donde se maneja de forma permanente información sensible o confidencial la cual debe ser protegida para salvaguardar la confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta los siguientes parámetros:

- La posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre.
- También se toman en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas que representan los edificios y zonas aledañas.

3.4.1.4. PI004. Título de la Política: Trabajo en áreas seguras - Ref.: ISO/IEC 27001 CL. A. 11.1.5

Definición de la Política:

Para garantizar la confidencialidad de la información se hace necesario establecer áreas seguras dentro de la entidad, por tal razón se deben establecer ciertos controles tanto para los funcionarios de la entidad , como para los terceros que tengan acceso a estas zonas de la entidad.

3.4.1.5. PI005. Título de la Política: Ubicación y protección de los equipos - Ref.: ISO/IEC 27001 CL. A. 11.2.1

Definición de la Política:

Los equipos deben ser ubicados y protegidos para salvaguardar la integridad y disponibilidad de la información, garantizándole el acceso únicamente al personal autorizado para su uso teniendo en cuenta los siguientes aspectos:

- Ubicar los equipos en zonas de la entidad donde se minimice el acceso de personal no autorizado.
- Ubicar las instalaciones de procesamiento y almacenamiento de información que contienen información confidencial o sensible, en una zona que permita la supervisión durante su uso.

3.4.1.6. PI006. Título de la Política: Servicios de suministro - Ref.: ISO/IEC 27001 CL. A. 11.2.2

Definición de la Política:

Los equipos deben estar protegidos con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía deberá estar de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

3.4.1.7. PI007. Título de la Política: Seguridad del cableado- Ref.: ISO/IEC 27001 CL. A. 11.2.3

Definición de la Política:

El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.

3.4.1.8. PI008. Título de la Política: Mantenimiento de equipos - Ref.: ISO/IEC 27001 CL. A. 11.2.4

Definición de la Política:

Se debe realizar el mantenimiento de los equipos para asegurar la continuidad de la operación y a su vez garantizar la disponibilidad e integridad de la información de forma continua, para lo cual es necesario realizar el mantenimiento preventivo a los equipos de la entidad, de acuerdo con los intervalos de servicio establecidos y atendiendo a las recomendaciones y especificaciones técnicas establecidas por el fabricante o el proveedor. La Oficina de TIC mantendrá un control actualizado

de la frecuencia de realización del mantenimiento preventivo de los equipos en la entidad.

3.4.1.9. PI009. Título de la Política: Escritorio limpio y pantalla limpia- Ref.: ISO/IEC 27001 CL. A. 11.2.9

Definición de la Política:

Se debe adoptar por parte de la Superintendencia del Subsidio Familiar una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información.

ELABORO		REVISO		APROBO	
Nombre:	Juan José Olivella	**Nombre:**		**Nombre:**	Norberto Agudelo Valencia
Cargo:	Profesional Universitario Oficina de Tecnologías de la Información y las Comunicaciones	**Cargo:**	Profesional Especializado Oficina de Tecnologías de la Información y las Comunicaciones	**Cargo:**	Jefe de Oficina de Tecnologías de la Información y las Comunicaciones
Fecha:	29/Sep./2015	**Fecha:**	29/Sep./2015	**Fecha:**	29/Sep./2015

MANUAL DE NORMAS DE SEGURIDAD DE LA INFORMACIÓN

SuperSubsidio
Vigilamos tu caja de compensación

Oficina de Tecnologías de la Información y las Comunicaciones

Calle 45 A # 9-46
Teléfonos: 3487777 - PBX: 3487800
Fax 3487804
www.ssf.gov.co - e-mail: ssf@ssf.gov.co
Bogotá D.C., Colombia

SuperSubsidio Vigilamos tu caja de compensación	**MANUAL DE NORMAS DE SEGURIDAD DE LA INFORMACIÓN**	CODIGO: MAN-GSI-YYY
		VERSION: 1
	Manual de Normas de Seguridad de la Información	FECHA: 29/Sep./2015

Contenido

Línea Gratuita Nacional 018000910110
Calle 45 A No. 9-46
Bogotá Colombia
Fax 3487804
ssf@ssf.gov.co

INTRODUCCIÓN

La base del presente manual es el documento MAN-GSI-XXX Manual de Políticas de Seguridad de la Información, el cual contiene los lineamientos en términos de seguridad definidos por la SSF. Dichos lineamientos fueron desarrollados de acuerdo a los requerimientos propios de la SSF para contrarrestar los riesgos detectados en el Análisis de Riesgos realizado en la Fase de Planear del SGSI.

Por otra parte, en el presente documento de Manual de Normas de Seguridad de la Información se establecen las acciones concretas a tomar para materializar el cumplimiento de las políticas definidas en el Manual de Políticas de Seguridad de la Información. De acuerdo a la definición y objetivo de cada una de las Normas que se definirán a continuación, estas pueden hacer el desarrollo de una o más políticas de seguridad. De la misma forma una política de seguridad puede ser desarrollada a través de varias normas de seguridad.

Este manual es elaborado con base en la norma ISO 27001:2013, el Marco de Referencia de Arquitectura Empresarial de MinTIC, el Modelo de Seguridad y Privacidad de la Información v 3.0 de MinTIC y los lineamientos de Gobierno en Línea (GEL).

1. PRESENTACIÓN DEL MANUAL

1.1. Objetivo de Manual

El presente Manual, tiene por objeto establecer las acciones que se deben ejecutar al interior de la SSF para dar cumplimiento a las políticas definidas en el documento MAN-GSI-XXX Manual de Políticas de Seguridad de la Información. Estas acciones se expresan mediante debes, procedimientos y guías que definen el tratamiento de los riesgos detectados en el análisis de riesgos de la Fase Planear del SGSI.

1.2. Alcance del Manual de Normas de Seguridad de la Información

El presente Manual de Normas de Seguridad de la Información es parte integral de todos los procesos de la Superintendencia de Subsidio Familiar y es de obligatorio cumplimiento por parte de todos los funcionarios y demás colaboradores de la entidad.

2. TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN

Los siguientes términos y definiciones están basados en el estándar NTC ISO/IEC 27001: 2013 y son aplicables a la Superintendencia del Subsidio Familiar y al PGSI de la misma:

Aceptación de riesgo: Decisión de asumir un riesgo.

Activo: cualquier elemento que represente valor para la organización.

Alta Dirección: Se considera Alta Dirección a los directivos con cargo más alto en una organización; el Presidente, el Gerente General y los Directores de las distintas áreas. En el caso de la Superintendencia del Subsidio Familiar se entiende como Alta Dirección a la integrada por la Superintendente y el Comité Directivo.

Análisis de Riesgo: Uso sistemático de la información para identificar fuentes y para estimar el riesgo (Guía ISO/IEC 73:2002).

Adaptabilidad: Define que todos los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes designados por la Alta Dirección con el objetivo de garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

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

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.

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

Dueño del riesgo sobre el activo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Información: Datos que poseen una información.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de

seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad d la información.

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

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Política: actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos.

Procedimiento: Forma especificada de llevar a cabo una actividad o un proceso.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Recursos informáticos: Todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimización del trabajo con computadores y periféricos, tanto a nivel Individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de los mismos.

Registro: Documento que presenta resultados obtenidos o proporcionar evidencia de actividades desempeñadas.

Responsable de Seguridad TIC: En LA ENTIDAD el comité de seguridad de la información será el grupo encargado de realizar el seguimiento y monitoreo al Sistema de Gestión de la Seguridad de la información (SGSI).

Responsables del Activo: Personas responsables del activo de información en el proceso.

Riesgo: El efecto de la incertidumbre sobre los objetivos". (Icontec, 2011, Pág.4)

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad. [NTC-ISO/IEC 27002:2013].

Sistema de gestión de la seguridad de la información SGSI: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales que se realicen en la entidad.

Tecnología de la Información: Se refiere al hardware y software operado por el organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

3. NORMAS DE SEGURIDAD DE LA INFORMACIÓN

Una norma de la seguridad de la información sustenta una política de seguridad y regula parte o la totalidad del objetivo de la misma.

Actualización de normas

Cualquier solicitud de modificación al documento de Políticas de Seguridad de la Información de la Superintendencia del Subsidio Familiar, debe ser realizada por el Comité de Seguridad de la Información.

Estructura de la Norma

La estructura de la Norma es la siguiente:

- Título de la norma
- Políticas relacionadas
- Objetivo
- Alcance
- Descripción

Reglas de escritura de las normas

- Las normas se escribirán en forma sencilla y en su texto indicarán que es una definición general y aplicable a la Superintendencia del Subsidio Familiar.
- El enunciado debe ser corto, bien redactado y conciso, además debe utilizarán términos y palabras que sean de uso común.

- Se mantendrán los términos de seguridad TIC definidos y expresados dentro del documento de seguridad TIC de la Superintendencia del Subsidio Familiar.

Codificación de las normas

- Las Normas de Seguridad de la Información con el prefijo **NA** son responsabilidad de la Administración de la Superintendencia del Subsidio Familiar según la NTC ISO/IEC 27001:2013.

- Las Normas de Seguridad de la Información con el prefijo **NTI** son responsabilidad de la Oficina de TIC de la Superintendencia del Subsidio Familiar según la NTC ISO/IEC 27001:2013.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.1. NA001. Roles y responsabilidades para la seguridad de la información

Políticas Relacionadas: PA003 Organización interna de la seguridad de la información, PA010 Terminación de contrato o cambio de responsabilidad en el empleo, PTI004 Propiedad de los activos, PTI005 Uso aceptable de los activos, PTI006 Devolución de activos, PTI044 Responsabilidades y procedimientos.

Objetivo: Definir las responsabilidades para la seguridad de la información que tienen las diferentes áreas dentro del Sistema de Gestión de Seguridad de la Información de la Superintendencia del Subsidio Familiar.

Alcance: Esta norma deberá ser adoptada por todos los colaboradores de la SSF que intervienen dentro del Sistema de Gestión de Seguridad de la Información de la entidad.

Descripción:

Responsabilidades

A continuación se presentan las responsabilidades de los principales elementos que intervienen en la construcción del Sistema de Gestión de Seguridad de la Información:

1. Responsabilidades de la Alta Dirección

La alta dirección debe promover el compromiso de todos los niveles de responsabilidad y autoridad de la SSF en la implementación de Sistema de Gestión de Seguridad de la Información. Para ello tiene las siguientes funciones específicas:

- Velar por el establecimiento de las políticas de seguridad de la información y los objetivos de seguridad alineados con las necesidades de la SSF
- Garantizar la integración de los lineamientos del SGSI con los procesos definidos en la SSF.
- Comunicar la necesidad de definir y mantener una gestión de la seguridad de la información representada por medio de los objetivos y las políticas de seguridad.
- Apoyar y promover a las personas para que contribuyan al desarrollo del SGSI y adquieran un rol de liderazgo en cada una de sus áreas de responsabilidad.
- Garantizar los recursos requeridos para el mantenimiento del SGSI.

2. Responsabilidades de la Oficina TIC

Es responsabilidad de la Oficina de TIC de la entidad:

- Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de seguridad de información.
- Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de información.
- Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de seguridad de la información.

- Diseñar, desarrollar, instalar y mantener las aplicaciones bajo su responsabilidad de acuerdo con la metodología establecida e incluyendo los controles de seguridad de información.

- Establecer, documentar y dar mantenimiento a los procedimientos de seguridad que apliquen para la plataforma de tecnologías de información administrada por esta oficina.

- Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.

- Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.

- Supervisar los procesos y/o actividades sobre las plataformas tecnológicas que manejen información de la SSF y que cuya administración se encuentre delegada en tercero.

- Implementar y administrar los controles de seguridad sobre los datos y conexiones de la red bajo su administración.

- Definir y gestionar programas de capacitación y entrenamiento que incluyan temas relevantes y pertinentes sobre seguridad de información.

- Custodiar la información y los medios de almacenamiento bajo su responsabilidad.

3. Responsabilidades de Gestión de riesgos de Seguridad de la Información

- Es responsabilidad de la Oficina Asesora de Planeación, con el apoyo del Oficial de Seguridad de la Información, llevar a cabo la Gestión de Riesgos de Seguridad de la Información en la SSF en concordancia con las políticas de seguridad y sus objetivos. Lo anterior se fundamenta en el Decreto 2595 de 2112, Artículo 6 Funciones de la Oficina Asesora de Planeación: …”7. Liderar y apoyar a las dependencias en la implementación, desarrollo y sostenimiento de sistemas integrados de gestión, de acuerdo a lo establecido en los planes y proyectos estratégicos de la Superintendencia.”

- El objetivo de la Gestión de riesgos es identificar y evaluar los riesgos de seguridad de la información a los cuales están expuestos los activos de la entidad, para seleccionar y aplicar el plan de tratamiento más adecuado. La evaluación de riesgos está basada en el impacto y probabilidad de ocurrencia de estos para la entidad y los requerimientos de los niveles de seguridad, tomando en cuenta los controles existentes.

- El análisis y evaluación de riesgos de seguridad debe hacerse al menos una vez al año.

- El detalle de la metodología de riesgos se encuentra en el documento MAN-GSI-XXX Metodología de Análisis de Riesgos de Seguridad de la Información (Basado en la metodología del SARO).

4. Responsabilidades de los propietarios de los riesgos (Lideres de los Procesos)

Es responsabilidad de los propietarios del riesgo:

- Clasificar sus activos de información de acuerdo con los requerimientos de confidencialidad, integridad y disponibilidad.

- Definir los requerimientos de continuidad y de recuperación en caso de desastre.

- Realizar un análisis anual de riesgos en conjunto con la oficina de riesgos, para determinar el grado de exposición a las amenazas vigentes y confirmar los requerimientos de confidencialidad, integridad y disponibilidad relacionados con sus activos de Información

- Definir los requerimientos de seguridad con el acompañamiento de la oficina de riesgos para los activos de información bajo su responsabilidad para que se les proporcione un nivel adecuado de protección en conformidad con los estándares, políticas y procedimientos de seguridad de información.

- Determinar y autorizar todos los privilegios de acceso a sus activos de información.

- Comunicar y gestionar al Oficial de Seguridad de la Información sus requerimientos en capacitación sobre seguridad de información.

- Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados a su proceso, incluyendo aquellas actividades que sean consideradas como controles de seguridad de la información dentro de dichos procedimientos.

5. Responsabilidades de funcionarios, contratistas y terceros

Es responsabilidad de los colaboradores (Funcionarios y Contratistas) y Terceros salvaguardar la información institucional de la entidad, garantizando así la confidencialidad, integridad y disponibilidad de la información teniendo como funciones:

- Cumplir fielmente las políticas de seguridad de la información, contempladas en el presente manual.
- Reportar, a la mayor brevedad posible y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de seguridad de información.
- Realizar sugerencias a la Alta Dirección para mejorar los procesos relacionados con los activos de información de la entidad y optimizar así el sistema de seguridad de la información.
- Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos indicados en las políticas de seguridad de la información.
- Incorporar la seguridad de información como parte de las actividades y tareas bajo su responsabilidad.
- Conocer las directrices de protección de los activos de información que utilicen.
- Utilizar únicamente software y demás recursos tecnológicos autorizados.

Clausulas aplicables a contratistas y terceros

Se debe coordinar con la Secretaria General y con la Oficina Asesora Jurídica la inclusión en los procesos de contratación las cláusulas de confidencialidad e integridad definidas en la presente norma, correspondientes a salvaguardar la confidencialidad e integridad de los activos de información de la SSF. En los

contratos que establezca la SSF con sujetos en los que estos tengan algún tipo de acceso a la información de la SSF, se deberán agregar las siguientes cláusulas:

- **Cláusula de Confidencialidad de la Información**: El Contratista se compromete a mantener la reserva de la información privilegiada y protegida que se le suministre y a no revelar tal información a terceras personas. Esto aplica adicionalmente al Tratamiento de Datos Personales antes, durante y después del contrato. En caso de incumplimiento de esta cláusula, se aplicará la normatividad aplicable, incluidas la Ley 734 de 2002 y la Ley 1273 de 2009.

- **Cláusula de Integridad de la Información**: El Contratista o Tercero debe conocer y aceptar las condiciones definas en la norma **NTI013 Integridad de la Información** descrita en el presenta documento, las cuales se refieren al manejo íntegro e integral de la información tanto interna como externa. Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

Código Disciplinario Único

En el caso de los funcionarios públicos en operación, estos deben conocer que sus contratos están sujetos a las responsabilidades implícitas en los deberes definidos en el Código Disciplinario Único - Ley 734 de 2002, en particular el Artículo 34 numeral 5: “Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos”.

Roles del SGSI

En el documento TIC-YYY-XXX “DEFINICIÓN DE LA ESTRUCTURA ORGANIZACIONAL PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN” se definen los Roles y Perfiles específicos del Sistema de Gestión de Seguridad de la Información (SGSI) para la SSF, los cuales deben ser adoptados e implementados al interior de la entidad, previa aprobación del documento en mención por parte del Comité de Seguridad de la Información. Dentro de los roles del SGSI se definen el comité de seguridad de la información, CIO, Oficial de seguridad, Coordinador de servicios, tecnológicos, Responsable de la Gestión de Proyectos en Sistemas de Información, entre otros.

Divulgación del Sistema de Gestión de Seguridad de la Información

Se debe adoptar lo descrito en el documento TIC-YYY-XXX “PLAN DE DIVULGACIÓN DE SEGURIDAD DE LA INFORMACIÓN” en el cual se establece

la línea base para llevar a cabo el proceso continuo de sensibilización a todos los colaboradores de la SSF resaltando la importancia de garantizar la Seguridad de la Información en todos los procesos al interior de la SSF y de esta manera mantener vigente y activo el SGSI.

Se debe crear y sistema continuo de divulgación del Sistema de Gestión de Seguridad de la Información de manera dinámica y actualizada conforme a los cambios tecnológicos y operativos que se vayan presentando en la SSF con el fin de lograr una permanente apropiación del SGSI en todos sus colaboradores.

3.2. NA002. Separación de deberes

Políticas Relacionadas: PA003 Organización interna de la seguridad de la información**,** PTI018 Separación de los ambientes de desarrollo, de pruebas y operación, PTI028 Separación de redes.

Objetivo: Realizar la correcta distribución de roles y responsabilidades, atendiendo a la debida segregación de funciones para reducir las oportunidades de una modificación no-autorizada y mal uso (intencional o no-intencional) de los activos de la organización.

Alcance: Esta norma define la manera de realizar la separación de deberes, roles o responsabilidades de los diferentes cargos en la Superintendencia del Subsidio Familiar, tanto para empleados como contratistas o terceros.

Descripción:

Cada área o dependencia de la entidad de manera autónoma e independiente de otras áreas, considerando que la segregación de los deberes es un método para reducir el riesgo de un mal uso accidental o deliberado del sistema, tiene el compromiso de que:

- El Oficial de Seguridad de la Información, en apoyo con el líder del proceso, debe mantener un inventario actualizado de los activos de información de cada área o dependencia y de acuerdo al grado de criticidad de dichos activos, el Oficial de Seguridad de la Información debe determinar la necesidad de realizar una segregación de funciones.

- Se deben identificar los riesgos asociados a modificación no-autorizada y mal uso (intencional o no-intencional) de los activos de información, provocada por una falta de separación de funciones. Dependiendo del nivel de riesgo detectado el Oficial de Seguridad de la Información debe determinar la necesidad de realizar una segregación de funciones.

- En casos en que sea difícil segregar funciones, el Oficial de Seguridad debe

considerar otros controles como el monitoreo de actividades y rastros de auditoría.

- Se deben efectuar y fortalecer los controles establecidos para la gestión efectiva de los riesgos asociados a la separación de funciones, conforme a las determinaciones del Comité de Seguridad. La implementación de estos controles debe realizarse de manera que se mantenga la independencia de las diferentes áreas de la SSF cuando ello amerite por razones de seguridad.

- Se debe aprobar y dar curso a las acciones de mejora establecidas en el Comité de Seguridad con la finalidad de llevar los niveles de riesgo asociados a la separación de funciones hasta los niveles aceptados por la entidad, según los criterios aplicados por el Oficial de Seguridad para la SSF.

- Se debe hacer seguimiento a las acciones de mejora con sus correspondientes controles de seguridad de la información aprobadas por el Comité de Seguridad, particularmente en lo referente a la separación de deberes.

- Se debe mantener el inventario actualizado de activos de información bajo la dirección del Oficial de Seguridad, de tal forma que se identifiquen aquellos que puedan requerir una segregación de funciones.

- A cargo del Oficial de Seguridad, se debe mantener actualizado el análisis de riesgos de seguridad donde se visibilicen aquellos provocados por una falta de segregación de funciones, de tal forma que se identifiquen aquellas actividades que puedan requerir una segregación de funciones.

3.3. NA003. Sensibilización.

Políticas Relacionadas: PA008 Toma de conciencia, educación y formación en la seguridad de la información.

Objetivo: Que los colaboradores de la SSF reciban una adecuada sensibilización en seguridad de la información y las actualizaciones regulares sobre las políticas y procedimientos establecidos por el SGSI para la entidad conforme sea relevante para su función laboral.

Alcance: Esta norma deberá ser considerada por toda persona que tenga un rol activo en el uso y protección de los activos de información, los cuales incluyen elementos hardware, elementos software, información física, información digital, personas, locaciones, etc. Es decir debe ir dirigida a todos los colaboradores de la

entidad.

Descripción:

- Se debe impartir la capacitación y el conocimiento a los colaboradores de la SSF a cargo del Oficial de Seguridad, para lo cual se debe comenzar con un proceso de inducción formal similar al descrito en el documento TIC-YYY-XXX "PLAN DE DIVULGACIÓN DE SEGURIDAD DE LA INFORMACIÓN", diseñado para introducir las políticas y expectativas de seguridad de la organización que afecten a la SSF, antes de otorgar acceso a la información o servicios.

- Debe programarse una capacitación constante cuya frecuencia la define el Comité de Seguridad de la SSF, la cual debe incluir los requerimientos de seguridad de información y responsabilidades legales, así como la capacitación en el uso correcto de los medios de procesamiento de información como por ejemplo, procedimiento de registro, uso de paquetes de software e información sobre los procesos disciplinarios.

- Las actividades de concientización, lideradas por el Oficial de Seguridad, deben ser adecuadas y relevantes para el rol, responsabilidades y capacidades del colaborador de la SSF. Deben incluir información sobre amenazas conocidas y establecer los canales apropiados para reportar los incidentes de seguridad de información.

- Con el debido cuidado a los aspectos de confidencialidad según el criterio del Oficial de seguridad, los incidentes en la seguridad de la información deben ser utilizados en la capacitación de los usuarios como ejemplos de lo que podría suceder, cómo responder ante tales incidentes y cómo evitarlos en el futuro.

- Cada colaborador de la Superintendencia del Subsidio Familiar debe participar de las sesiones de sensibilización sobre seguridad en la información, según lo defina la Oficina de TIC y la Coordinación de Desarrollo Humano de la Superintendencia del Subsidio Familiar.

- Se debe realizar un proceso continuo de talleres de sensibilización en seguridad de la información para todos los colaboradores de la SSF bajo la supervisión del Oficial de Seguridad, basados en lo descrito en el documento TIC-YYY-XXX "PLAN DE DIVULGACIÓN DE SEGURIDAD DE LA INFORMACIÓN", resaltando la importancia de garantizar la Seguridad de la Información en todos los procesos al interior de la SSF y de esta manera mantener vigente y activo el SGSI.

- Se debe hacer periódicamente presentaciones magistrales guiadas por el Oficial de Seguridad, mediante ayudas didácticas de manera que se logre en el público la apropiación de la información presentada y una efectiva generación de conocimiento, mediante la experiencia de hechos cotidianos relacionados con la seguridad de la información de la SSF, tomando como modelo, lo descrito al respecto en el documento TIC-YYY-XXX "PLAN DE DIVULGACIÓN DE SEGURIDAD DE LA INFORMACIÓN".

- Se debe plantear en las capacitaciones, casos críticos con ejemplos de situaciones reales. Las sesiones de sensibilización deben estar apoyadas en casos prácticos que se evidencian al interior de la SSF y que tengan relación directa con los activos de información más críticos identificados en la entidad, conforme a las pautas descritas en el documento TIC-YYY-XXX "PLAN DE DIVULGACIÓN DE SEGURIDAD DE LA INFORMACIÓN"

- Se debe hacer uso de material gráfico, con el apoyo de la Oficina de Comunicaciones de la SSF, como posters y fondos de pantalla lo cual aporta a la estrategia de divulgación una mayor capacidad de recordación para los colaboradores de la SSF.

- Se deben establecer procesos de retroalimentación, guiados por el Oficial de Seguridad, acerca de las sensibilizaciones realizadas.

Administración de Seguridad

3.4. NTI001. Perfiles de Acceso

Políticas Relacionadas: PA020 Privacidad y protección de información de datos personales, PTI008 Política de control y Administración de accesos, PTI009 Seguridad para Internet, PTI010 Seguridad para redes inalámbricas, PTI011 Administración de cuentas, PTI016 Gestión de cambios, PTI026 Control de redes, PTI027 Seguridad de los servicios de red.

Objetivo: Evitar el acceso no autorizado a los servicios de la red, regulando la creación, asignación, cambios y retiros de perfiles de acceso.

Alcance: Esta norma define la manera en que se crea, otorga, cambia y se inactivan los perfiles de acceso que poseen los colaboradores, a los distintos recursos tecnológicos de la Superintendencia del Subsidio Familiar.

Descripción:

Se debe garantizar el acceso de los usuarios a las redes y los servicios de red sin comprometer la seguridad de la información, para lo cual la SSF debe tener en cuenta los siguientes lineamientos técnicos:

- Se deben aplicar los mecanismos AAA (Authentication, Authorization and Accounting), apropiados para todos los colaboradores de la SSF que deban ingresar a los ambientes de administración de los dispositivos de comunicaciones o servidores, mediante el uso de aplicaciones como Radius o Tacacs y el Directorio Activo. Es responsabilidad del Oficial de Seguridad el llevar a cabo su implementación con el apoyo del Coordinador de Servicios Tecnológicos.
- Se debe seguir el **procedimiento de creación y cancelación de cuentas de usuario** de acuerdo a los criterios establecidos en el Comité de Seguridad en cabeza del Oficial de Seguridad, el cual está elaborado con base a los siguientes lineamientos:

  - Los usuarios sólo deben tener acceso a los servicios para los cuales hayan sido específicamente autorizados.

  - El procedimiento de creación y cancelación de cuentas de usuario debe tener cobertura a todas las redes y servicios de la SSF.

  - Los mecanismos de autenticación y autorización automática de usuarios para acceso a los servicios de la SSF es responsabilidad del Oficial de Seguridad con el apoyo del Coordinador de servicios Tecnológicos y debe tener los siguientes lineamientos:

    - Las credenciales de autenticación básicas son: nombre de usuario, contraseña y dirección de tarjeta de red del computador. Esto obliga a que el usuario solo ingrese a los sistemas de información desde su equipo de trabajo.
    - Las credenciales de los usuarios en lo posible deber ser gestionadas por medio de un Directorio Activo, permitiéndose otros esquemas de acuerdo al criterio del Oficial de Seguridad de la Información.

  - Se deben identificar los requerimientos de autenticación y autorización orientados al acceso y uso de las aplicaciones misionales y de apoyo de la SSF de manera individual consultando los fabricantes, proveedores, desarrolladores y/o responsables de estas aplicaciones en la medida de sus niveles de criticidad para la entidad. Esta labor debe estar encabezada por el Oficial de Seguridad con la colaboración del Responsable de Gestión de Proyectos y del Coordinador de Servicios Tecnológicos.

  - Se debe tener en cuenta que los perfiles de usuario deben estar ajustados a niveles de privilegio estrictos de acuerdo a los sistemas que use por razones del desempeño de sus funciones de tal manera que no le sea posible ingresar a otros campos de información de la entidad para

evitar el incumplimiento normativo como el habeas data personal, habeas data financiero, la ley de transparencia, etc.

- Se debe establecer un protocolo para realizar la solicitud formal de los permisos de acceso a los sistemas de información cuyo conducto regular establecido en la SSF, mediante los formatos respectivos y emanados por la oficina de gestión documental de la SSF es: usuario – jefe directo – director de oficina TIC – responsable del sistema autorizador.

- Se debe revisar de manera periódica en la SSF (cada seis meses), el procedimiento de creación y cancelación de cuentas de usuario con el fin de identificar posibles riesgos, proponer planes de mejoramiento e implementar o reforzar controles de seguridad de la información.

- Los criterios para revocar los derechos de acceso son los siguientes: vencimiento del contrato de trabajo, uso inadecuado del activo de información, traslado del colaborador a otra área de trabajo o incumplimiento de algunas de las condiciones definidas en el manual de políticas del SGSI de la SSF.

- Es responsabilidad de la oficina encargada de implementar el procedimiento de creación y cancelación de cuentas de usuario, el definir, asignar y mantener actualizados los perfiles de acceso a la información en cada una de las aplicaciones de acuerdo con las funciones del colaborador.

- A partir de la fecha de creación de este documento y con el fin de poder lograr una seguridad homogénea y altamente administrable, los sistemas de información que se desarrollen o adquieran deben diseñarse de forma tal que permita la administración de perfiles.

- Se debe Inventariar la totalidad de los usuarios, identificar los servicios y aplicaciones que utilizan, revisar la validez de los permisos actuales de acceso y aplicar los permisos de acuerdo a los criterios de seguridad apropiados según el cargo de cada usuario.

3.5. NTI002. Acceso Controlado a Terceros sobre Recursos Tecnológicos

Políticas Relacionadas: PA012 Seguridad de la información para las relaciones con proveedores, PA013 Tratamiento de la seguridad dentro de los acuerdos con proveedores, PA020 Privacidad y protección de información de datos personales, PTI008 Política de control y Administración de accesos, PI001 Perímetro de

seguridad física, PI002 Controles de Accesos Físicos.

Objetivo: Gestionar los riesgos a la información y a las instalaciones de procesamiento de información que existen en los procesos donde se involucra a Terceros, de acuerdo a los requerimientos institucionales y de seguridad para el acceso a los recursos tecnológicos de la SSF.

Alcance: Aplica a todas las actividades de acceso a información de la SSF que involucren terceros.

Descripción:

Donde exista la necesidad de permitir a una empresa contratista o a un tercero el acceso a las instalaciones de procesamiento de la información o la información de la SSF, el Oficial de Seguridad de la Información debe llevar a cabo una evaluación del riesgo que le permita identificar los controles de seguridad requeridos para proteger la información conforme a la actividad que va a desarrollar el contratista o Tercero. Para esto se deben tener en cuenta los siguientes lineamientos:

- Se deben determinar las instalaciones de procesamiento de información o la información de la SSF a la cual el contratista o Tercero necesita tener acceso.

- Se debe identificar el tipo de acceso que tendrá el contratista o Tercero a la información y las instalaciones de procesamiento de información:

    - Acceso físico: Implica acceso directo a las locaciones de la SSF, por ejemplo: oficinas, edificios de cómputo, archivadores.
    - Acceso lógico: Implica acceso directo a la información digital de la SSF, por ejemplo: bases de datos o sistemas de información de la SSF.
    - Conectividad a la red: Implica acceso por medio de equipos conmutadores de red, por ejemplo, conexión permanente local, acceso remoto por canal dedicado, acceso por VPN en teletrabajo, etc.

- Para el caso de acceso a la red de la SSF (cableada o inalámbrica) por parte de un tercero, se deben definir y usar protocolos de comunicación seguros que garanticen la confidencialidad e integridad de la información transferida.

- Se debe informar al contratista o tercero acerca de los riesgos de seguridad involucrados en el acceso físico, lógico o de conectividad a la red, según corresponda.

- Se debe implementar tanto en conexiones de red físicas como inalámbricas, un mecanismo de autenticación mediante el servidor 802.1x, el cual valida los usuarios y proporciona acceso a la red. Adicionalmente, el acceso inalámbrico debe realizarse mediante protocolo de autenticación WPA2-Enterprice en el punto de acceso y autenticando en un servidor 802.1x.

- Se debe determinar el nivel de criticidad de la información expuesta ante el contratista o Tercero y su grado de importancia para las operaciones misionales o de apoyo.

- Se debe identificar el personal del Tercero involucrado en el manejo de la información de la SSF.

- Se deben conocer los diferentes medios y controles empleados por el Tercero cuando almacena, procesa, comunica, comparte e intercambia información.

- Se debe crear una red destinada al uso del personal contratista o tercero de manera que se pueda controlar y monitorear el acceso a otras redes donde se maneja información confidencial para la SSF.

- Se debe estipular en el contrato los requerimientos legales y reguladores y otras obligaciones contractuales asociadas a seguridad de la información para llevar cabo la labor del contratista o tercero. Esto conforme a lo definido en la norma **NA001. Roles y responsabilidades para la seguridad de la información,** en la sección de Clausulas aplicables a contratistas y terceros.

3.6. NTI003. Monitoreo

Políticas Relacionadas: PA003 Organización interna de la seguridad de la información, PTI004 Propiedad de los activos, PTI021 Registro de eventos, PTI044 Responsabilidades y procedimientos.

Objetivo: Producir y mantener registros de auditoría de las actividades y eventos de seguridad de la información durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso de modo que se detecten las actividades de procesamiento de información no autorizadas.

Alcance: Esta norma contempla las actividades de monitoreo que incluye la revisión de registros de eventos de los roles que ejecuta cada servidor, donde se almacenan registros, alarmas o errores, para la toma de acciones preventivas o correctivas.

Descripción:

- Se deben implementar plataformas de monitoreo, bajo el control de Administrador de Red, que permitan hacer seguimiento al comportamiento de la red de comunicaciones, servidores, aplicaciones y usuarios. De esta manera se disminuyen los riesgos que puedan afectar la disponibilidad e integridad de la información.

- Los registros de monitoreo sobre el manejo de la información de la SSF deben ser analizados por el Administrador de los Sistemas de Seguridad y deben incluir, cuando sea relevante, los siguientes elementos como evidencias para su posterior análisis o para reportes de auditoría:

    - Nombres de usuario o IDs.
    - Fechas, horas y detalles de eventos claves; por ejemplo, ingreso y salida.
    - Identificación o ubicación del dispositivo que accede a la información, si es posible.
    - Intentos de acceso fallidos y rechazados al sistema.
    - Intentos de acceso fallidos y rechazados a los datos y otros recursos.
    - Actividades realizadas por el usuario
    - Nivel de privilegio o perfil de usuario.
    - Utilidades y aplicaciones del sistema empleadas.
    - Archivos a los cuales se tuvo acceso y los tipos de acceso.
    - Direcciones y protocolos de la red.

- Adicionalmente se deben tener registros de monitoreo asociados a cambios en la configuración del sistema, alarmas activadas por el sistema de control de acceso, activación y desactivación de los sistemas de protección como sistemas antivirus y sistemas de detección de intrusiones. El análisis de estos registros debe estar a cargo del Administrador de los Sistemas de Seguridad.

- Dado, que los registros de auditoría pueden contener datos personales confidenciales, se deben mantener las medidas de protección de privacidad apropiadas de acuerdo a la Ley 1581 de 2012 sobre Protección de Datos Personales.

- Los administradores del sistema no deben tener permiso para borrar o desactivar los registros de sus propias actividades.

3.7. NTI004. Tratamiento de Incidentes de Seguridad

Políticas Relacionadas: PA008 Toma de conciencia, educación y formación en la seguridad de la información, PTI005 Uso aceptable de los activos, PTI044 Responsabilidades y procedimientos, PTI045 Reporte de eventos de seguridad de la información, PTI046 Evaluación de eventos de seguridad de la información y decisiones sobre ellos, PTI047 Aprendizaje obtenido de los incidentes de seguridad de la información, PTI048 Recolección de evidencia, PTI050 Implementación de la continuidad de la seguridad de la información.

Objetivos: Asegurar que los eventos y debilidades de la seguridad de la información sean comunicados de manera que permita realizar una acción correctiva oportuna. Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

Alcance: Esta norma alcanza a todo elemento lógico o físico que se conecte a la Red de la Superintendencia del Subsidio Familiar.

Descripción:

- Se deben establecer procedimientos formales de reporte y del progreso de un evento. Todos los colaboradores de la SSF deben tener el conocimiento adecuado de los procedimientos que manejan para que reporten los diferentes tipos de eventos y/o debilidades que podrían tener un impacto en la seguridad de los activos de la SSF.

- Se debe reportar cualquier evento o debilidad de la seguridad de la información lo más rápidamente posible al canal apropiado, por ejemplo a la Mesa de Ayuda de la SSF, para lo cual es necesario implementar un sistema de gestión de incidentes automatizado donde los usuarios puedan reportar los diferentes eventos de seguridad de la información, los responsables de atender estos eventos deben canalizarlo rápidamente para su atención y dar una solución oportuna conforme a unos Acuerdos de Niveles de Servicio (ANS) definidos.

- Se debe asegurar que el punto de contacto para reportar incidentes de la seguridad de la información sea conocido a través de toda la organización, que siempre esté disponible y sea capaz de proporcionar una respuesta adecuada y oportuna.

- Los procedimientos de reporte deben incluir:

    - Procesos de retroalimentación adecuados para asegurar que aquellos que reportan eventos en la seguridad de la información sean notificados

de los resultados después de haber tratado y solucionado el problema.
- Formatos de reporte de eventos que afecten la seguridad de la información para documentar el incidente y hacer posterior trazabilidad.
- La referencia al Código Disciplinario Único (Ley 734) en particular el Artículo 34 numeral 5: "Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos".

- La Oficina de TIC de la Superintendencia del Subsidio Familiar debe coordinar la implementación y ajuste de los controles adecuados conforme al resultado de análisis de riesgos realizado en el PGSI y el tratamiento de incidentes de seguridad de la información que sucedan en la SSF.

- Se deben revisar los informes o reportes periódicos de eventos sucedidos a los servidores, aplicativos y equipos de comunicaciones a fin de detectar posibles anomalías y establecer acciones correctivas y de mejora.

- Se debe llevar un registro documental en la base de datos de conocimiento donde se guarden las soluciones encontradas a los incidentes como lecciones aprendidas para que sirva de apoyo al soporte de incidentes.

3.8. NTI005. Separación de Ambientes y Funciones

Políticas Relacionadas: PA003 Organización interna de la seguridad de la información, PTI016 Gestión de cambios, PTI028 Separación de redes.

Objetivo: Reducir los riesgos de acceso y manipulación no autorizada a los ambientes de producción de la SSF, con el fin de garantizar una operación correcta de las instalaciones de procesamiento de información.

Alcance: Esta norma regula la separación de ambientes que deberá existir en la infraestructura tecnológica a fin de proveer una segregación de funciones.

Descripción:

- Para controlar la seguridad en las redes, el Administrador de Red debe crear dominios de red lógicos separados. En la Oficina TIC de la SSF se deben tener al menos los siguientes dominios o ambientes de red: ambiente de desarrollo, ambiente de pruebas y ambiente de producción.

- A nivel de la SSF, el Administrador de Red debe crear dominios de red lógicos separados por áreas: Oficina Asesora de Planeación, Oficina Asesora Jurídica, Oficina TIC, Oficina de Control Interno, Oficina de

Protección y Atención al Usuario, Secretaría General y las Superintendencias Delegadas.

- Los dominios de red establecidos y su interrelación deben ser configurados por el Administrador de Red de acuerdo a una evaluación del riesgo realizada por el Oficial de Seguridad de la Información y a los requerimientos de seguridad de cada uno de los dominios. Se deben implementar los controles de acceso adecuados a los diferentes dominios de red conforme a los niveles de privilegio de los diferentes usuarios

Se reconocen los siguientes ambientes básicos en la oficina TIC:

- Ambiente de Desarrollo: En este dominio de red se tienen los elementos hardware y software necesarios para que los colaboradores expertos en desarrollo de sistemas de información y demás servicios de apoyo a la SSF realicen sus actividades sin afectar la producción de la entidad.

- Ambiente de Pruebas: Una vez se hace el desarrollo del sistema de información o aplicación, se deben realizar las pruebas correspondientes. En este ambiente se tienen los elementos hardware y software necesarios para realizar las pruebas a los aplicativos o sistemas de información desarrollados internamente por la SSF o contratados a un tercero. Dichas pruebas son necesarias a fin de constatar que los sistemas realizan correcta e integralmente los requerimientos para los que fueron creados. Este debe ser un ambiente estable, con modificaciones o cambios controlados. Para pasar un sistema, módulo o programa de éste ambiente al de producción debe existir una aprobación formal por parte del funcionario responsable del área involucrada en las pruebas que actúa como cliente de la aplicación o sistema de información y del jefe de la Oficina de TIC. Si se requiere, en este ambiente se deben utilizar datos de prueba y nunca datos de producción.

- Ambiente de Producción: Es el ambiente donde se utilizarán y transformarán los datos de la Superintendencia del Subsidio Familiar, por lo tanto es el ambiente donde residirá la información operativa de la Entidad. No se permite efectuar pruebas sobre este ambiente a excepción de la primera implementación de cada software.

3.9. NTI006. Software Adquirido

Políticas Relacionadas: PTI025 Restricciones sobre la instalación y/o actualización de software.

Objetivo: Establecer procedimientos para controlar la instalación de software en los sistemas operativos, y regular la adquisición de cualquier tipo de software para la Superintendencia del Subsidio Familiar.

Alcance: Esta norma contempla todo tipo de software a ser adquirido en la Superintendencia del Subsidio Familiar: Sistema operacional, bases de datos, software de comunicaciones, utilitarios del sistema, software de seguridad, software de monitoreo, software de oficina y software aplicativo, entre otros.

Descripción:

Para minimizar el riesgo de corrupción de los sistemas operativos, se deben establecer los siguientes lineamientos de acuerdo al Procedimiento de Control de Cambios:

- La actualización del software operacional, aplicaciones y bibliotecas de programas sólo debe ser realizada por el administrador del sistema operativo o el personal de la mesa de ayuda, previa aprobación del director de la oficina TIC.

- El software de las aplicaciones y el sistema operativo sólo se debe implementar después de una prueba extensa y satisfactoria incluyendo: pruebas de utilidad, pruebas de seguridad, impacto sobre los sistemas de información y facilidad para el usuario. Estas validaciones deben estar supervisadas por el Responsable de la Planeación y Ejecución de Pruebas apoyado en la Mesa de Ayuda.

- Se debe hace uso de una base de datos del conocimiento donde se depositen todas las licencias, manuales y plantillas de configuración de los diferentes dispositivos de cómputo, desde PCs, servidores, equipos de comunicaciones y de seguridad de manera que se tenga un control y gestión centralizado de todo el software empleado en la SSF. Se debe mantener un inventario actualizado de licencias de software de la SSF, como parte de la política PTI003 Inventario de Activos.

- Se debe establecer una estrategia de “regreso a la situación original” (rollback) antes de implementar los cambios.

- Se debe mantener un registro de auditoría de todas las actualizaciones.

- Para efectos de concientización y divulgación, se deben hacer capacitaciones sobre las restricciones en la instalación de software a nivel de la entidad, conforme a los lineamientos dados en el documento XXX-YYY "PLAN DE DIVULGACIÓN DE SEGURIDAD DE LA INFORMACIÓN".
- Para garantizar conformidad con los estándares de seguridad de información propios, se debe adquirir hardware y software a través de canales autorizados, para lo cual se deben tener identificados dichos canales.

- Todo el software de la Entidad debe ser legalmente adquirido y se debe contar con las respectivas licencias que lo demuestren.

- Está prohibido para los empleados de la Superintendencia del Subsidio Familiar descargar y/o instalar cualquier tipo de software. Todas las solicitudes de instalación o configuración de software deben ser dirigidas hacia la mesa de ayuda de la SSF.

- Todo software a instalarse en las estaciones de trabajo debe estar licenciado.

3.10. NTI007. Utilización de claves de Acceso

Políticas Relacionadas: PTI008 Política de control y Administración de accesos, PTI012 Política de Gestión de contraseñas, PTI013 Política sobre el uso de controles criptográficos (Protección de la Información), PTI014 Gestión de llaves.

Objetivo: Que el manejo de claves secretas en la SSF sea interactivo, se creen claves secretas adecuadas para la seguridad de la entidad y se regule el uso y características de las claves de acceso.

Alcance: Esta norma define todos los parámetros genéricos que deben poseer las claves de acceso y el mantenimiento que los clientes internos deben llevar a cabo con las mismas.

Descripción:

- Un sistema de gestión de claves secretas debe cumplir con los siguientes lineamientos:

    - Hacer uso de IDs de usuarios individuales y claves secretas para establecer responsabilidades.
    - El directorio activo no debe permitir repetir claves y debe obligar cambio de primer ingreso automáticamente.

- Permitir a los usuarios seleccionar y cambiar sus propias claves secretas e incluir un procedimiento de confirmación para permitir errores de input.
- La clave secreta debe ser robusta: longitud mínima de ocho caracteres, combinar mayúsculas, minúsculas, números y símbolos. No se deben utilizar palabras sencillas en cualquier idioma, nombres propios, lugares, combinaciones excesivamente cortas, fechas de nacimiento, etc.
- La clave secreta se debe cambiar al menos cada tres meses, para la cual el sistema debe forzar su caducidad.
- Obligar a los usuarios a cambiar las claves secretas temporales en su primer ingreso o registro.
- Mantener un registro de claves de usuario previas y evitar el re-uso, al menos de 10 contraseñas.
- No mostrar las claves secretas en la pantalla en el momento de ingresarlas.
- Almacenar los archivos de claves secretas separadamente de los datos del sistema de gestión de claves la SSF.
- Almacenar y transmitir las claves secretas en un formato protegido (por ejemplo, cifrado).

- La contraseña es privada, confidencial e intransferible, siendo su titular responsable de evitar su divulgación quien, ante la presunción de que otra persona pudiera conocerla, debe proceder a cambiarla inmediatamente. Se considerará causa grave y será sancionado de acuerdo al Código Disciplinario Único (Ley 734 como se describe en la Norma NA001 del presente documento), el hecho de revelar a otra persona su propia contraseña o solicitar la contraseña de otro usuario.

- Se deben modificar todas las contraseñas que traen los equipos (Hardware y Software) por defecto una vez estos se hayan instalados

Seguridad del Software y Hardware

3.11. NTI008. Perfiles de Acceso

Políticas Relacionadas:

Objetivo: Regular la definición, instalación y mantenimiento de los parámetros de seguridad de la infraestructura tecnológica de la Superintendencia del Subsidio Familiar.

Alcance: Esta norma contempla todos aquellos parámetros relacionados directa o indirectamente con la seguridad de la infraestructura tecnológica de la Entidad.

Descripción:

- La homologación de hardware o software a instalar en la Entidad, permite que este sea incorporado respetando los estándares establecidos, logrando de esta forma homogeneidad en los parámetros relativos a la seguridad, permitiendo un control de la infraestructura tecnológica, la facilidad de mantenimiento y monitoreo.

- La Oficina de TIC será el responsable de la homologación del hardware y software mediante un proceso de revisión de los parámetros de seguridad vigentes.

- Es responsabilidad de la Oficina de TIC de la Superintendencia del Subsidio Familiar mantener actualizado el manual de estándares de seguridad cuando se incorpore una nueva tecnología.

- Para modificar los estándares establecidos, se debe justificar técnicamente la necesidad, determinar el alcance de la modificación y evaluar el impacto desde el punto de vista de seguridad, con el fin de determinar si debe ser acompañado por otras medidas. Posteriormente y en caso de ejecutarse la modificación, debe registrarse en el formato de control de cambios e implementarse las medidas pertinentes sobre todos los equipos de idénticas características.

3.12. NTI009. Protección de Hardware y Software de Seguridad

Políticas Relacionadas: PTI005 Uso aceptable de los activos, PTI012 Gestión de contraseñas, PTI018 Separación de los ambientes de desarrollo, de pruebas y operación, PTI021 Registro de eventos, PTI022 Protección de la información de registro, PTI025 Restricciones sobre la instalación y/o actualización de software, PTI027 Seguridad de los servicios de red.

Objetivo: Regular la protección del hardware y software de seguridad.

Alcance: Esta norma abarca a cualquier hardware y software que se utilice exclusivamente para la seguridad de cualquier ambiente, infraestructura, o sistema instalado en la Superintendencia del Subsidio Familiar, ya sea adquirida o de desarrollo propio.

Descripción: Cualquier hardware y software que sea utilizado exclusivamente con fines de seguridad y control, independientemente de su naturaleza, complejidad o modo de adquisición, debe cumplir las siguientes reglas:

- Los activos que hagan parte del hardware y software de seguridad en la SSF, deberán estar a cargo de un responsable, que será el Oficial de Seguridad de la Información quien a su vez delegará la custodia y gestión al administrador de los sistemas de seguridad.

- Cualquier uso indebido o mal funcionamiento del Hardware y Software de seguridad en la SSF deberá ser reportado inmediatamente por cualquier usuario dentro de la organización siguiendo el procedimiento de gestión de incidentes.

- Las credenciales de acceso a la gestión del Hardware o Software de seguridad sólo deben ser manejadas por el administrador de los sistemas de seguridad, y por ningún motivo serán divulgadas a terceros, teniendo en cuenta PTI012 Política de Gestión de contraseñas.

- El Oficial de Seguridad de la Información debe definir, y el administrador de los sistemas de seguridad debe implementar y gestionar, los elementos de Hardware y software de seguridad que garanticen la separación de ambientes de desarrollo, pruebas y operación, teniendo en cuenta el Procedimiento de paso de ambientes de desarrollo y pruebas a ambientes de producción.

- Los registros de eventos provenientes del Hardware y el Software de seguridad de la SSF, deberán conservarse en un lugar seguro con acceso restringido al personal autorizado y con protección de acceso.

- El software de seguridad debe ser utilizado exclusivamente para la Superintendencia del Subsidio Familiar.
- No se podrá desactivar, modificar, instalar versiones diferentes, ni realizar ninguna otra actividad que modifique el comportamiento del hardware y software de seguridad, sin llevar a cabo lo definido en el documento PR-GSI-XXX Procedimiento de Gestión de Cambios, con la expresa autorización del Oficial de Seguridad de la Información y la formal supervisión de las actividades de alteración.

- La documentación, manuales y cualquier otro tipo de información técnica sobre su comportamiento deben residir en la Oficina de TIC bajo la responsabilidad del Administrador de los Sistemas de Seguridad y/o el Oficial de Seguridad de la Información.

- Ninguna persona podrá transmitir en modo formal o informal, información alguna sobre los parámetros, variables y modo de instalación de ninguna herramienta de seguridad.

3.13. NTI010. Uso de Equipos Asignados por la entidad

Políticas Relacionadas: PTI004 Propiedad de los activos, PTI005 Uso aceptable de los activos, PTI006 Devolución de los activos. PA011 Clasificación de la información

Objetivo: Regular el uso de los equipos de la Superintendencia del Subsidio Familiar asignados a sus colaboradores.

Alcance: Esta norma cubre todo equipo de cómputo de uso interno de la Entidad que interactúe con la infraestructura tecnológica de la Superintendencia del Subsidio Familiar.

Descripción:

- Se constituye como una falta gravísima por parte de un colaborador de la SSF el atentar contra la inviolabilidad de la correspondencia y demás formas de comunicación. Lo anterior conforme al numeral 16 del artículo 48 (Faltas Gravísimas) de la Ley 734 de 2002 que define el Código Disciplinario Único.

- Todo software residente en un equipo de cómputo o estación de trabajo debe protegerse contra alteraciones a su ejecución, que puedan provocar ataques de elevación de privilegios, robo o modificación de información o acceso no autorizado, etc., para lo cual se deben configurar controles técnicos (por ejemplo software antivirus, software anti rootkit, HIPS (Host Intrusion Prevention System), etc.) que prevengan esta situación.

- Todo instalador de software aprobado por la Oficina TIC debe copiarse antes de iniciar su uso, y esas copias deben almacenarse en un lugar seguro y confiable. Estas copias originales no deben usarse para actividades comerciales ordinarias, sino que deben reservarse para cuando se presenten infecciones de virus, daños en el disco duro y otros problemas en los equipos de cómputo.
- Se debe desarrollar de forma regular un plan de divulgación en seguridad de la información (ver documento TIC-YYY-XXX “PLAN DE DIVULGACIÓN DE SEGURIDAD DE LA INFORMACIÓN) que propenda por socializar la presente norma referida al uso adecuado de los activos de información de la SSF, incluidos los equipos de cómputo designados y los datos a los cuales se tenga acceso.

- El acceso y distribución de la información de la Superintendencia del Subsidio Familiar se regulará de acuerdo a lo definido en el documento XXX-YYY-ZZZ **Guía de Clasificación y Etiquetado de la Información** dependiendo de la fuente de la cual se solicita.

- La **Guía de Clasificación y Etiquetado de la Información** define los niveles de clasificación de la información definidos para la SSF e identifica el tipo de información (bases de datos, archivos de texto, imágenes o cualquier otro tipo de archivo institucional) perteneciente a cada nivel.

Parámetros y condiciones para el uso de los equipos designados por la entidad:

- El colaborador de la SSF a quien le ha sido asignado un equipo o estación de trabajo tiene el rol de custodio del mismo y por ende debe salvaguardarlo de forma adecuada y velar por la integridad del mismo. Lo anterior conforme al numeral 21 y 22 del artículo 34 (Deberes de todo servidor público) de la Ley 734 de 2002 que define el Código Disciplinario Único.

- Todos los colaboradores de la SSF deben devolver todos los activos de la organización que le han sido asignados o que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

- El colaborador de la SSF debe utilizar los bienes asignados (equipo o estación de trabajo) para el desempeño de su empleo, cargo o función o la información reservada a la que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos. Lo anterior conforme al numeral 4 del artículo 34 (Deberes de todo servidor público) de la Ley 734 de 2002 que define el Código Disciplinario Único.

- Se constituye como una falta gravísima por parte de un colaborador de la SSF el causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar, o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas. Lo anterior conforme al numeral 43 del artículo 48 (Faltas Gravísimas) de la Ley 734 de 2002 que define el Código Disciplinario Único.

- Los colaboradores de la Superintendencia del Subsidio Familiar no podrán instalar ningún programa o software no autorizado por la Oficina TIC en los equipos o estaciones de trabajo asignados.

- Los colaboradores de la Entidad no podrán almacenar información clasificada como **reservada** o **confidencial** en el disco duro del equipo personal o estación de trabajo, a menos que la Oficina TIC tenga conocimiento y disponga de las medidas de protección adecuadas.

- Si un colaborador en ejercicio de sus funciones debe almacenar información clasificada como **reservada** o **confidencial** en su estación de trabajo debe

informar al Oficial de Seguridad de la Información para que este defina en función de la situación las medidas de protección adecuadas.

- Los equipos y estaciones de trabajo de la SSF no deben moverse o reubicarse sin la aprobación previa del Jefe de la Oficina de TIC de la Entidad o quien el delegue para este propósito.

3.14. NTI011. Copias de Respaldo de Software y Datos de Seguridad

Políticas Relacionadas: PTI005 Uso aceptable de los activos, PTI016 Gestión de cambios, PTI017 Gestión de capacidad, PTI020 Respaldo de información, PTI021 Registro de eventos, PTI022 Protección de la información de registro, PTI029 Transferencia de información, PTI038 Control de cambios en el sistema, PI002 Controles de Acceso Físico.

Objetivo: Regular la toma de respaldos del software y datos de seguridad.

Alcance: Esta norma abarca a cualquier módulo de control de acceso, herramienta y/o software de seguridad y sus archivos de datos.

Descripción: La Oficina de TIC de la Superintendencia del Subsidio Familiar definirá, para los sistemas y archivos involucrados en la seguridad, los siguientes aspectos:

- La información contenida en los servidores se respalda de forma periódica
- Los medios de las copias de seguridad se almacenan localmente y en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.
- Las copias de seguridad son probadas periódicamente para garantizar la integridad de la información almacenada y que pueda ser recuperada oportunamente.
- Para garantizar que la información de los funcionarios, contratistas y demás terceros autorizados sea respaldada, es responsabilidad de cada uno mantener copia de la información que se maneje en el recurso compartido definido para cada área y/o usuario
- Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información de la entidad deben ser etiquetados de acuerdo a la información que almacenan haciendo alusión a su contenido.

- Los medios de almacenamiento con información crítica o copias de respaldo son manipulados única y exclusivamente por el personal encargado de hacer los respaldos y su salvaguarda.

- El Oficial de Seguridad de la Información debe definir el esquema de backups adecuado (tipo de backup, frecuencia, medio de almacenamiento, etc.) para la información a respaldar.

3.15. NTI012. Cifrado de Datos

Políticas Relacionadas: PA020 Privacidad y protección de información de datos personales, PTI013 Política sobre el uso de controles criptográficos (Protección de la Información).

Objetivo: Regular la utilización de los métodos de cifrado de información de la Superintendencia del Subsidio Familiar.

Alcance: Esta norma buscará regular la utilización de los métodos de cifrado a ser utilizados por la Superintendencia del Subsidio Familiar en los canales de comunicaciones.

Descripción: Deben utilizarse métodos de cifrado en los casos en que se requiera que la información de la Superintendencia del Subsidio Familiar a ser transmitida mediante canales de comunicación, no sea leída o modificada por personas no autorizadas.

El cifrado de documentos puede llevarse a cabo en las siguientes situaciones:

- En la transmisión de información **confidencial** o **reservada** de la entidad hacia entidades o personas externas.

- Cuando haya un acuerdo de confidencialidad con otra entidad o persona sobre la información que se va a transmitir.

- Cuando el propietario del riesgo o el Oficial de Seguridad de la Información consideren que se trata de un activo de información critico basado en una valoración de riesgo.

El uso de controles criptográficos con el fin de garantizar el No Repudio puede llevarse a cabo en las siguientes situaciones:

- Cuando se busque un mecanismo de trazabilidad de las acciones sobre la información de la SSF (creación, recepción, entrega, etc.).

- Cuando se establezca la necesidad de implementar procesos de intercambio electrónico de información con garantía de no repudio.

Se definen los siguientes lineamientos para la administración de controles criptográficos:

- Siempre se deben proteger los equipos de cómputo utilizados para la operación de los controles criptográficos, especialmente en los casos de generación, validación y revocación de llaves criptográficas.

- El Oficial de Seguridad de la Información debe identificar los equipos de cómputo en los cuales se realiza procesamiento de información cifrada y establecer los mecanismos de protección adecuados para garantizar la confianza en los controles criptográficos.

- Los métodos de cifrado designados por la SSF para ser utilizados en el aseguramiento de la confidencialidad de la información o en la gestión de la seguridad en sistemas de información se encuentran definidos en el documento XXX-YYY-ZZZ **Guía de Clasificación y Etiquetado de la Información.** Este documento define los niveles de clasificación de la información de la SSF e identifica las condiciones técnicas de manejo para cada nivel.

- En los casos en los que se realice un proceso de cifrado de la partición del sistema operativo o de todo el disco duro se debe crear un disco de recuperación (Rescue Disk) que permita restaurar el disco cifrado en caso de que se dañe el gestor de arranque, la llave maestra o el sistema operativo. Esto no evita la necesidad de poseer la correcta contraseña para el descifrado.

- En caso de pérdida de información cifrada, el usuario debe reportar tal situación como un incidente de seguridad de la información mediante el documento PR-GSI-XXX Procedimiento de Gestión de Incidentes. De esta forma el Oficial de Seguridad de la Información evaluará si existe un medio (por ejemplo un disco de recuperación) para hacer la recuperación de la información.

- La gestión de llaves o contraseñas asociadas a cualquier usuario de red o de sistema de información debe llevarse a cabo, cuando sea posible, utilizando la arquitectura de directorio activo existente en la SSF. Esto implica que en la medida de lo posible la autenticación de los usuarios debe hacerse contra el directorio activo. De esta forma se evita manejar bases de datos de contraseñas dispersas y no gestionadas.

- La generación y almacenamiento de claves para el caso de usuarios nuevos debe ser definida en el documento PR-GSI-XXX Procedimiento de Creación y cancelación de cuentas de usuario.

- La administración de claves para el caso de usuarios existentes, por ejemplo en situaciones de cambio de claves, se debe resolver mediante una solicitud de soporte incluida en el documento PR-GSI-003 Procedimiento de Soporte y Atención a Solicitudes.

3.16. NTI013. Integridad de la Información

Políticas Relacionadas: PA011 Clasificación de la información, PTI004 Propiedad de los activos, PTI027 Seguridad de los servicios de red, PTI029 Transferencia de la información, PTI030 Acuerdos sobre transferencia de información, PTI031 Mensajería electrónica.

Objetivo: Regular la definición y alcance de los controles que garanticen la integridad de la información.

Alcance: Esta norma contempla todos los equipos de cómputo que procesen información de la Superintendencia del Subsidio Familiar, sean o no de su propiedad y la información transmitida de una fuente a otra con o sin procesamiento.

Descripción:

Se establecen los siguientes apartados tendientes a preservar la integridad de la información de la SSF:

- Con el fin de garantizar la integridad de la información por parte de los colaboradores de la SSF, se debe establecer un compromiso para el manejo integro de la información interna y externa que se debe incluir en los contratos mediante una cláusula de integridad de la información.

- El Oficial de Seguridad de la Información deberá apoyar la generación de la cláusula de integridad de la información en conjunto con la Oficina Asesora Jurídica, y realizar las actualizaciones correspondientes en función de las necesidades de la SSF.

- Con el fin de garantizar la integridad de la información de la SSF, esta debe ser transferida interna y externamente por medio de los canales oficiales establecidos por la Oficina TIC, especialmente aquellos establecidos para la mensajería electrónica y la transferencia de grandes volúmenes de datos.

- La información de la SSF debe ser entregada de forma íntegra y coherente únicamente a las personas a quien esta va dirigida. Igualmente la modificación de la información de la SSF solo se permitirá bajo autorización del propietario o responsable de dicha información. Generalmente el propietario de la información es el líder del proceso en el cual la información es generada o custodiada.

- El Oficial de Seguridad de la Información debe definir los controles de seguridad necesarios a implementar para garantizar la integridad de la información en cualquiera de sus estados: En uso (por parte del usuario final o por parte de un proceso en un servidor), en movimiento (en tránsito en la red LAN o WAN) o en reposo (cuando esta almacenada).

Adicionalmente se definen los siguientes controles de seguridad a implementar:

- **Revisión del ingreso de información:** Todo sistema o programa, debe poseer los controles necesarios que garanticen que la información se ingrese en su totalidad de forma precisa, completa y de acuerdo con los tiempos establecidos.

- **Revisión del procesamiento de la información:** Todo sistema o programa, debe poseer los controles necesarios que garanticen que la información es procesada en su totalidad de forma completa, exacta y en el período estipulado.

- **Autenticación:** En los sistemas que procesan, transmiten o gestionan información se deben implementar mecanismos de autenticación de usuario o procesos con el fin de identificar adecuadamente al actor que manipula la información de la SSF. El proceso de autenticación debe llevarse a cabo (en la medida de lo posible) a través de la arquitectura de directorio activo de la SSF.

- **Autorización**: En los sistemas que procesan, transmiten o gestionan información se deben implementar mecanismos de autorización de usuario o procesos con el fin de asegurar que las actividades de manipulación de la información se encuentran autorizadas.

3.17. NTI014. Prevención y Detección de Virus

Políticas Relacionadas: PTI019 Controles contra códigos maliciosos.

Objetivo: Minimizar la pérdida de datos y software a través del ataque de virus informático.

Alcance: Esta norma abarca todo el software de la infraestructura tecnológica y aplicaciones de la Superintendencia del Subsidio Familiar susceptibles de ser atacados por virus informáticos.

Descripción:

En la infraestructura tecnológica que contenga sistemas operativos o aplicaciones, deben implantarse soluciones que detecten y neutralicen ataques provocados por códigos maliciosos. Para ello se deben tener en cuenta los siguientes lineamientos:

- Se debe configurar una regla general para todas las estaciones de trabajo, equipos portátiles y equipos servidores que evite la descarga de cualquier archivo ejecutable. El Oficial de Seguridad de la Información determinará los equipos exentos de esta regla considerando algunas funciones propias de la SSF que sobre estos se desarrollen por ejemplo: equipos en los que se haga desarrollo, instalación o pruebas de software.

- En la medida de lo posible se debe configurar y desplegar una solución que regule la ejecución de aplicaciones en estaciones de trabajo, equipos portátiles y equipos servidores a aquellas que se encuentran dentro un inventario de aplicaciones autorizadas por la SSF. Si no se dispone de una herramienta de validación automática, se debe auditar de forma regular los equipos de la SSF para corroborar el cumplimiento de este punto.

- Se debe configurar la actualización periódica del conjunto de aplicativos dispuestos contra códigos maliciosos, lo cual incluye la actualización del software así como de los datos requeridos por el software para poder operar tales como base de datos de virus o firmas.

- Se debe configurar la ejecución periódica de un proceso de búsqueda (Scanning) de código malicioso intensivo en los equipos en los cuales se tenga desplegada una solución de antivirus.

- El Oficial de Seguridad de la Información determinará la necesidad de instalar software contra códigos maliciosos en equipos celulares, dado que estos contienen información relevante de la entidad, especialmente aquellos que contengan el buzón de correo corporativo.

- El Oficial de Seguridad de la Información debe velar porque se lleve a cabo un proceso regular de actualización de parches de seguridad en los sistemas de información de la SSF.

- El Oficial de Seguridad de la Información debe revisar periódicamente el conjunto de software instalado en los equipos de procesamiento de información que sustentan los procesos críticos de la SSF, identificando la presencia de virus o modificaciones no autorizadas en los mismos.

- Se deben configurar las soluciones contra códigos maliciosos instaladas para verificar la presencia de virus en archivos recibidos de fuentes externas o a través de redes no confiables.

- El Oficial de Seguridad de la Información, con apoyo del Jefe de la Oficina TIC, debe liderar un proceso de concientización a los colaboradores de la SSF en la adopción de diferentes actitudes preventivas frente a virus informáticos que eviten un daño hacia la Entidad, entre ellas verificar el remitente de la información antes de abrirla o ejecutarla.

3.18. NTI015. Respaldo de Información

Políticas Relacionadas: PTI003 Inventario de activos, PTI004 Propiedad de los activos, PTI008 Política de control y Administración de accesos, PTI020 Respaldo de la información.

Objetivo: Garantizar que la información de la SSF sea respaldada en un medio confiable y que sea recuperable cuando se necesite.

Alcance: Esta norma contempla todo tipo de información manejada por los colaboradores de la SSF entre las cuales están:

- Datos de las aplicaciones.
- Sistemas de información (programas fuentes y objetos).
- Software de la infraestructura tecnológica.
- Información Técnica.
- Información contenida en los servidores.
- Bases de Datos.

Descripción:

- El Oficial de Seguridad de la Información debe definir el esquema de los backups de la información de la SSF, considerando, la frecuencia de backup, el tamaño de la información, la criticada otorgada, el medio de almacenamiento, entre otros aspectos relacionados:
    - La información valorada con una disponibilidad o integridad alta, de acuerdo a la metodología para la identificación de activos deberá tener copias de seguridad, diaria incremental, semanal total y mensual total.

- La información valorada con una disponibilidad o integridad media, de acuerdo a la metodología para la identificación de activos deberá tener copias de seguridad, semanal total y mensual total.
- La información valorada con una disponibilidad o integridad baja de acuerdo a la metodología para la identificación de activos deberá tener copias de seguridad mensual total.

- El custodio de la información es el encargado de hacer el respaldo de información, siguiendo el procedimiento XXX de ejecución de backups.

- Todos los respaldos de información tienen la misma criticidad de los activos a respaldar. Por lo tanto, ese valor de criticidad es el que define el esquema de backups a aplicar de acuerdo a lo definido en el punto 1 de la presente norma.

- Se debe registrar en detalle todas las copias de respaldo a la información de la SSF que se ejecutan actualmente, indicando el tipo, la periodicidad, la fecha de creación y el periodo de retención, teniendo en cuenta el procedimiento de ejecución de backups.

- Todos los respaldos de información deben ser retenidos de acuerdo a lo establecido por las tablas de retención documental y la regulación correspondiente, y deben ser almacenados en un sitio seguro que garantice su confidencialidad, integridad y disponibilidad.

- Es responsabilidad del Oficial de Seguridad de la Información, validar que se realice un respaldo de pruebas cada tres meses, el cual e realiza seleccionando aleatoriamente uno de los respaldos de información que se encuentran registrados.

Seguridad de las comunicaciones

3.19. NTI016. Accesos Remotos

Políticas Relacionadas: PTI005 Uso aceptable de los activos, PTI008 Política de control y Administración de accesos, PTI009 Seguridad para Internet, PTI011 Administración de cuentas, PTI012 Política de Gestión de contraseñas, PTI013 Política sobre el uso de controles criptográficos (Protección de la Información), PTI027 Seguridad de los servicios de red.

Objetivo: Especificar el uso de accesos remotos a los recursos informáticos e información de la Superintendencia del Subsidio Familiar.

Alcance: Esta norma contempla todos los accesos remotos que se establezcan con la Red Interna de la Superintendencia del Subsidio Familiar.

Descripción:

- Todo acceso remoto que se haga a los recursos informáticos de la Superintendencia del Subsidio Familia se otorgará siguiendo el procedimiento de creación y cancelación de cuentas de usuario que tendrá que ser previamente autorizado por el Oficial de Seguridad de la Información.

- Los usuario que utilicen accesos remotos deberán hacer uso del mismo únicamente para el propósito al cual fue concedido, por ningún motivo se podrá acceder a información o sistemas que no sean parte de los permisos solicitados y autorizados según el procedimiento de creación y cancelación de cuentas de usuario.

- Los parámetros y las credenciales de acceso de los usuarios que se utilizarán en los accesos remotos deberán ser suministrados por el administrador de los sistemas de seguridad.

- El Oficial de Seguridad de la Información deberá evaluar previamente la viabilidad del acceso remoto al recurso informático teniendo en cuenta la criticidad del activo y los factores que puedan afectar la seguridad de la conexión.

- Por ningún motivo se podrá compartir las credenciales de acceso remoto asignadas para una conexión con otro usuario o tercero según lo manifiesta PTI012 Política de Gestión de contraseñas.

- Las conexiones realizadas a través del protocolo RDP deberán utilizar mecanismos de cifrado adecuados conforme al documento XXX Guía de Clasificación y Rotulación de la Información y usar mecanismos de autenticación NLA (Network Layer Authentication).

- El Oficial de Seguridad de la Información deberá implementar mecanismos perimetrales en el firewall destinados a proteger las conexiones de acceso remoto.

- El Oficial de Seguridad de la Información deberá implementar a todas las conexiones túneles VPN para cualquier acceso remoto.

3.20. NTI017. Seguridad Internet

Políticas Relacionadas: PTI005 Uso aceptable de los activos, PTI009 Seguridad para Internet, PTI019 Controles contra códigos maliciosos, PTI027 Seguridad de los servicios de red

Objetivo: Definir los aspectos de seguridad que debe aplicar la Superintendencia del Subsidio Familiar para la protección de la información de la Entidad en el uso del servicio de Internet.

Alcance: Esta norma contempla cualquier tipo de comunicación que se establezca a través del servicio de Internet por parte de los colaboradores de la Superintendencia del Subsidio Familiar desde equipos pertenecientes a la Red interna para la realización de tareas operativas.

Descripción: Para el acceso a Internet, los funcionarios, contratistas y demás personas que hagan uso del servicio, deben tener en cuenta los siguientes aspectos:

- El servicio de internet debe usarse exclusivamente para las actividades propias de la función desarrollada en la entidad y no debe utilizarse para ningún otro fin, teniendo en cuenta la política PTI005 Uso aceptable de los activos.

- Los usuarios autorizados para acceder al servicio de internet en la SSF son los responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la entidad.

- El oficial de seguridad es responsable de monitorear el tráfico y las comunicaciones establecidas en el servicio de internet de la SSF, para evitar las vulnerabilidades que puedan afectar la información de la entidad.

- Por ningún motivo el servicio de internet puede ser usado para descarga de información masiva de gran tamaño que pueda llegar a colapsar la red.

- Por ningún motivo el servicio de internet debe ser usado para descargar o visualizar información y contenidos que atenten contra la seguridad de la información de la SSF según lo contemplado en la política PTI019 Controles contra códigos maliciosos.

- El Oficial de Seguridad de la Información deberá monitorear el nivel de seguridad en los servicios de red que soporta el servicio de internet, teniendo en cuenta la política PTI027 Seguridad de los servicios de red.

- Los usuarios no podrán acceder a páginas relacionadas con pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, pornografía, spyware, adware, redes peer to peer (p2p), juegos, apuestas online, entre otras, que se encuentren fuera del contexto laboral.

- Acceder a Internet por el canal contratado y aprobado por la entidad. No se autoriza hacer conexiones no controladas ni limitadas hacia Internet.

- No se permitirá la descarga, uso, intercambio y/o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.

- Informar en caso de recibir información en archivos adjuntos de dudosa procedencia o que no se esté esperando, al Oficial de Seguridad de la entidad, quién escalará el incidente de seguridad a quién corresponda al interior de la entidad, para analizar y evitar la materialización de cualquier tipo de riesgo que afecte cualquier activo de información.

- Las conexiones directas de salida a internet no están permitidas, sin pasar por un firewall o un proxy.

- No se permite la conexión de módems externos o internos, que no estén autorizados por el Oficial de Seguridad de la Información.

Seguridad Física

3.21. NTI018. Seguridad Física - Dispositivos de Seguridad Contra Incidencias

Políticas Relacionadas: PTI003 Inventario de activos, PTI008 Política de control y Administración de accesos, PI001 Perímetro de seguridad física, PI002 Controles de accesos Físicos, PI005 Ubicación y protección de los equipos, PA015 Seguimiento y revisión de los servicios de los proveedores.

Objetivo: Definir el tipo y características de los dispositivos de seguridad contra incidencias que posee el Centro de Datos de la Superintendencia del Subsidio Familiar.

Alcance: Esta norma regula la instalación de dispositivos en el Centro de Datos de la Entidad.

Descripción: En el Centro de Datos de la Superintendencia del Subsidio Familiar, deben existir dispositivos de seguridad que garanticen la detección temprana de incidencias consideradas como mínimas a controlar.

Para tal efecto se debe tener en cuenta los siguientes aspectos:

- La Superintendencia del Subsidio Familiar es responsable del impacto que puedan provocar los incidentes en los Centros de datos a cargo de terceros, según la política PA015 Seguimiento y revisión de los servicios de los proveedores.

- Debe existir un sistema de detección y prevención de incendios en el Centro de datos, que minimice el impacto que puede generar la ocurrencia de un evento o situación de incendio en el lugar. Así mismo, se debe contar con un sistema de control de acceso que permita registrar el ingreso del personal.

- Debe existir un sistema de refrigeración en el centro de datos de la Superintendencia del Subsidio Familiar, que sea capaz de enviar alarmas vía correo electrónico al oficial de seguridad, en caso de mal funcionamiento o futuro mantenimiento.

- Debe existir un sistema de regulación y estabilización del fluido eléctrico, el cual debe comunicar y alarmar eventos relacionados con la energía al Oficial de Seguridad de la Información.

- Es responsabilidad del Oficial de Seguridad de la Información proteger y velar por el mantenimiento físico y lógico de los dispositivos y sistemas de seguridad contra incidencias.

3.22. NTI019. Seguridad Física –Backups

Políticas Relacionadas: PTI003 Inventario de activos, PTI008 Política de control y Administración de accesos, PTI020 Respaldo de la información. PI001 Perímetro de seguridad física, PI002 Controles de accesos Físicos, PI003 Seguridad de las oficinas, recintos e instalaciones, PI005 Ubicación y protección de los equipos,

Objetivo: Definir los controles de acceso físico que deben existir en los lugares donde se resguarden los backups de la SSF.

Alcance: Esta norma define los controles de seguridad física instalados en los lugares donde se guardan dispositivos que almacenan los backups de la SSF.

Descripción: Adicionalmente a las medidas de control de acceso y dispositivos de control de incidencias ya descritas en las normas de seguridad física respectiva, debe tenerse en cuenta los siguientes aspectos:

- Los respaldos deben ser almacenados en un sitio suficientemente seguro de la SSF que les permita mantener su integridad ante la ocurrencia de un desastre en las instalaciones. En los casos de activos críticos el Oficial de Seguridad de la Información determinará si los respaldos de la información deben ser almacenados en un sitio externo a la SSF.

- Los respaldos deben ser almacenados en la cintoteca destinada para tal fin donde solo se permita el acceso a personas autorizadas según lo indica la política PTI008 Política de control y Administración de accesos.

- El lugar de custodia de la cintoteca no debe estar rodeado de condiciones ambientales que puedan deteriorar los respaldos, como fluidos, humedad, temperatura. De igual manera, el lugar debe contar con detectores de humo y sistemas de detección de incendios.

- Es responsabilidad del Jefe de la Oficina de TIC de la Entidad el constatar con una periodicidad adecuada que los dispositivos que alertan el estado ambiental del lugar donde se encuentra la cintoteca.

- Esta norma debe estar incluida en la parte pertinente en el documento de Plan de Contingencia de la Superintendencia del Subsidio Familiar.

- Todos los cambios estructurales dentro de los lugares destinados al almacenamiento de soportes magnéticos deben ser informados al jefe de la Oficina de TIC de la Entidad a fin de que se evalúe antes de la realización de los mismos las posibles consecuencias sobre la seguridad física establecida.

Gestión de Incidentes de Seguridad de la Información

3.23. NTI020 Responsabilidades y procedimientos

Políticas Relacionadas: PTI044 Responsabilidades y procedimientos (Gestión de incidentes de seguridad de la información), PTI045 Reporte de eventos de seguridad de la información, PTI046 Evaluación de eventos de seguridad de la información y decisiones sobre ellos, PTI047 Aprendizaje obtenido de los

incidentes de seguridad de la información, PTI048 Recolección de evidencia.

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Alcance: Esta norma define las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información

Descripción: La Gestión de Incidentes de seguridad de la información se llevará de acuerdo al documento PR-GSI-XXX Procedimiento de Gestión de Incidentes de Seguridad, según las siguientes etapas:

- **Detección o reporte del incidente:** Los colaboradores de cada área son los encargados de reportar al Oficial de Seguridad de la Información sobre los incidentes presentados en su área, con el fin de gestionarlos, mitigando así el impacto que los incidentes generan. La oficina TIC puede considerar implementar un sistema de gestión de incidentes automatizado que facilite al usuario el reporte de los incidentes.

  Adicionalmente, el Oficial de Seguridad de la Información, con apoyo del jefe de la Oficina TIC, debe definir y liderar la implementación de los mecanismos adecuados para la detección de incidentes de seguridad asociados a cualquiera de los estados de la información: En uso (por parte del usuario final o por parte de un proceso en un servidor), en movimiento (en tránsito en la red LAN o WAN) o en reposo (cuando esta almacenada).

  Igualmente se deben revisar los informes o reportes periódicos de eventos sucedidos a los servidores, aplicativos y equipos de comunicaciones a fin de detectar posibles anomalías y en caso de que aplique reportar un incidente de seguridad de la información.

- **Análisis del incidente reportado:** El Oficial de Seguridad de la Información debe clasificar el tipo de incidente y establecer su prioridad de acuerdo al Procedimiento de Gestión de Incidentes. Esto con el objetivo de dar prioridad a aquellos incidentes que se cataloguen como críticos dentro de la entidad. Igualmente se debe identificar si el incidente ocasionó el incumplimiento a alguna normatividad aplicable, incluidas la Ley 1273 de 2009 o la Ley 734 de 2002 - Código Disciplinario Único.

- **Recolección de evidencia:** El Oficial de Seguridad de la Información debe liderar el proceso de recolección de evidencia forense del incidente en cado de que se requiera con el fin de utilizar dicha información como prueba en caso de que se dé una acusación formal contra el atacante o sus cómplices,

de acuerdo a lo indicado como hecho punible en la Ley 1273 de 2009 o la Ley 734 de 2002 - Código Disciplinario Único.

- **Contención o preparación de la solución del incidente:** Acorde con la prioridad en la que se clasifique el incidente se deben establecer medidas de mitigación inmediatas con el fin de gestionar el mismo. Estas son medidas de choque para evitar aumentar el impacto, hasta cuando se establece una acción definitiva para mitigar el incidente de forma definitiva.

- **Solución del incidente:** Para dar una solución eficaz al incidente se debe evaluar y analizar la información de incidentes similares que se hayan presentado en la entidad. A continuación el Oficial de Seguridad de la Información debe definir la solución más adecuada para el incidente y debe generar un conjunto de actividades a realizar con sus respectivos responsables con el fin de erradicar el incidente generado.

- **Recuperación y seguimiento del incidente:** Se debe hacer seguimiento a las actividades implementadas para erradicar el incidente de seguridad y se deben evaluar los resultados de forma conjunta entre el colaborador que reporta el incidente y el Oficial de Seguridad de la Información. Si se considera que las actividades realizadas gestionaron adecuadamente el incidente se procederá a su cierre, si por el contrario no se gestionó de forma adecuada se vuelve a plantear una nueva solución.

- **Registro y comunicación del incidente:** El Oficial de Seguridad de la Información debe llevar un registro documental del incidente de seguridad con el fin de garantizar la trazabilidad sobre los mismos al igual que para permitir aprender de ellos y utilizar la información histórica para la toma de decisiones en incidentes futuros. Adicionalmente el Oficial de Seguridad de la Información debe informar a la persona que realizó el reporte del incidente acerca de cómo se atendió y resolvió.

3.24. NTI021. Reporte de eventos de seguridad de la información.

Políticas Relacionadas: PTI044 Responsabilidades y procedimientos (Gestión de incidentes de seguridad de la información), PTI045 Reporte de eventos de seguridad de la información, PTI046 Evaluación de eventos de seguridad de la información y decisiones sobre ellos, PTI047 Aprendizaje obtenido de los incidentes de seguridad de la información, PTI048 Recolección de evidencia.

Objetivo: Definir los canales de gestión para el reporte rápido y oportuno de los eventos de Seguridad de la Información.

Alcance: Esta norma define los canales de gestión apropiados para el reporte de eventos de Seguridad de la Información.

Descripción:

- El Oficial de Seguridad de la Información, con el apoyo del área que realice las funciones de comunicación organizacional dentro de la SSF, debe liderar el proceso de socialización de los canales autorizados para el reporte de eventos de seguridad de la información.

- Todos los colaboradores de la SSF y terceros deben reportar al Oficial de Seguridad de la Información o al Jefe de la Oficina TIC cualquier evento de seguridad observado o sospechado, entendido como una situación en la cual posiblemente se ve afectada la confidencialidad, integridad o disponibilidad de la información.

- Todos los colaboradores de la SSF y terceros, que utilicen los sistemas y servicios de información de la SSF deben reportar al Oficial de Seguridad de la Información o al Jefe de la Oficina TIC cualquier debilidad de seguridad observada o sospechada en el sistema o en los servicios que son utilizados en la entidad.

- Los canales autorizados para el reporte de eventos o debilidades de seguridad de la información son los siguientes: 1) Vía correo electrónico: osi@ssf.gov.co, joti@ssf.gov.co 2) Vía llama telefónica: 3 487800 ext. 7906.

- La SSF debe disponer de una función de soporte de respuesta a incidentes que preste asistencia a los usuarios de sus sistemas de información para el reporte y el manejo de los incidentes de seguridad. En cualquier caso el incidente reportado debe ser gestionado de acuerdo al documento PR-GSI-XXX Procedimiento de Gestión de Incidentes de Seguridad.

- Todos los eventos de seguridad reportados que sean considerados incidentes de seguridad dado que efectivamente comprometen la confidencialidad, integridad o disponibilidad de los activos de información de la SSF, serán investigados y se les hará seguimiento de acuerdo al Procedimiento de Gestión de Incidentes por parte del Oficial de Seguridad de la Información.

Gestión de la Continuidad del Negocio

3.25. NTI022. Planificación de la continuidad de la seguridad de la información

Políticas Relacionadas: PTI049 Planificación de la continuidad de la seguridad de la información.

Objetivo: Incluir en los sistemas de gestión de la continuidad del negocio de la entidad, la continuidad de la seguridad de la información.

Alcance: Esta norma define los requisitos definidos por la SSF para asegurar la continuidad de la seguridad de la información en situaciones adversas.

Descripción: Se establece un plan de continuidad con el fin de restaurar la operación en un tiempo prudencial después de generada la falla o interrupción, garantizando así la disponibilidad de la información, para tal fin se deben considerar las siguientes actividades:

- Se debe hacer una identificación de los procesos más críticos de la entidad, los cuales impacten de forma directa los objetivos misionales y sobre estos definir y construir un Plan de Continuidad de Negocio.

- Se debe documentar los riesgos que enfrenta la SSF en términos de la probabilidad y el impacto de perder disponibilidad de recursos tecnológicos críticos, con el objetivo de identificar y determinar la prioridad de los procesos críticos de la entidad.

- El Oficial de Seguridad de la Información con el apoyo del área que realice las funciones de comunicación organizacional dentro de la SSF, debe realizar el proceso de divulgación de Plan de Continuidad de Negocio a todos los colaboradores de la SSF.

- Todas las áreas de la SSF se deben comprometer en la implementación del Plan de Continuidad de Negocio. Los dueños de las unidades de negocio son los responsables de mantener documentados y actualizados los procesos a su cargo e informar cualquier cambio al responsable de la gestión del Plan de Continuidad de Negocio, que en este caso es el Oficial de Seguridad de la Información.

- Dentro de las estrategias y procedimientos de recuperación a desarrollar en el marco del Plan de Continuidad de Negocios se debe asegurar la continuidad de la seguridad de la información y en ningún caso se debe

anteponer la urgencia en la recuperación de la operación sobre la seguridad de los activos de información de la SSF.

- Se debe establecer e implementar procedimientos de recuperación para permitir la reanudación de las operaciones de la entidad y garantizar la disponibilidad de la información de la SSF.

- Se debe definir e implementar estrategias de recuperación tecnológica necesarias para garantizar la continuidad de los procesos críticos.

- Se debe identificar y asignan roles y responsabilidades a los colaborares de la SSF y terceros dentro del Plan de Continuidad de Negocios que defina la entidad.

- Los niveles de recuperación tecnológica mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados, deben estar incorporados y definidos en el Plan de Continuidad de Negocio.

3.26. NTI023. Implementación de la continuidad de la seguridad de la información

Políticas Relacionadas: PTI050 Implementación de la continuidad de la seguridad de la información.

Objetivo: Establecer procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información.

Alcance: Esta norma define los controles necesarios para asegurar la continuidad del negocio en la entidad ante situaciones adversas.

Descripción: Para la etapa de implementación del plan de continuidad se debe tener en cuenta los siguientes criterios:

- La Oficina de TIC debe mantener los procedimientos y controles establecidos en el marco del Plan de Continuidad de Negocio, con el fin de garantizar que estos se mantengan operantes y efectivos.

- La Oficina de TIC debe hacer pruebas y simulaciones para establecer el nivel de efectividad del Plan de Continuidad de Negocio de la SSF, evaluando el tiempo del restablecimiento y de recuperación de la disponibilidad de la información: RTO (Tiempo objetivo de recuperación) y RPO (Punto objetivo de recuperación).

- Se debe capacitar a los colaboradores de la SSF y a terceros que tienen

responsabilidades en el Plan de Continuidad de Negocio, mediante pruebas o simulacros.

- La Oficina de TIC debe realizar pruebas de recuperación técnica, para asegurar que los sistemas de procesamiento de información puedan restablecerse de manera efectiva y de acuerdo a los tiempos RTO y RPO definidos en el Plan de Continuidad de Negocio.

- La SSF debe coordinar con los proveedores incluidos dentro de la estrategia de recuperación de la SSF, las pruebas de restablecimiento de los servicios prestados por parte de los proveedores de la entidad para asegurar de que los servicios provistos externamente se restablezcan de forma adecuada.

- La SSF debe realizar pruebas completas, para establecer que toda la entidad en su conjunto puede restablecer la operación en los tiempos definidos en al Plan de Continuidad de Negocio.

3.27. NTI024. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Políticas Relacionadas: PTI051 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Objetivo: Verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados

Alcance: Esta norma define el monitoreo y seguimiento realizado a los controles de continuidad de la seguridad de la información establecidos e implementados.

Descripción: Los acuerdos de continuidad del negocio deben ser probados periódicamente, utilizando simulaciones realistas (que implican tanto a los usuarios como al personal de la Oficina de TIC), para demostrar si el personal es capaz de recuperar la información crítica y los sistemas dentro de escalas de tiempo críticas.

- La SSF debe evaluar periódicamente el Plan de Continuidad de Negocio y debe realizar la actualización correspondiente si lo considera necesario.

- Posterior a la activación del Plan de Continuidad del Negocio definido por la SSF y cuando se logre la etapa de normalización, se debe hacer una revisión de la acciones emprendidas para establecer su grado de eficacia en el restablecimiento de la operación y la forma como se garantizó la disponibilidad de la información.

- Se debe documentar el resultado de las acciones emprendidas dentro del Plan de Continuidad de Negocio y los resultados obtenidos en la restauración, recuperación y normalización de la operación de la SSF.

3.28. NTI025. Disponibilidad de instalaciones de procesamiento de información

Políticas Relacionadas: PTI052 Disponibilidad de las instalaciones de procesamiento de información.

Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de información de la SSF con el fin de cumplir los requisitos de disponibilidad de la Entidad.

Alcance: Esta norma define los controles necesarios a nivel de infraestructura tecnológica para satisfacer los requisitos de disponibilidad de la SSF.

Descripción:

- Las instalaciones de procesamiento de información (principales o alternas) deben estar en condiciones físicas y ambientales propicias para garantizar la correcta ejecución y restablecimiento de las operaciones cuando sea necesario. Esto impacta directamente la integridad y disponibilidad de la información de la SSF.

- En caso de que se tenga contratado el uso de infraestructura, plataforma hardware, o software remoto (por ejemplo en un centro de datos principal/ alterno o a través de una solución de computación en la nube), el supervisor de dicho contrato debe validar la existencia de acuerdos de nivel de servicios (ANS) que definan de forma clara las condiciones del servicio, que incluyen: disponibilidad porcentual, MTBF (Mean Time Between Failure), efectividad en la instalación, efectividad en la ampliación de capacidades (elasticidad y flexibilidad), efectividad en la atención de solicitudes, calidad de los reportes entregados, servicios de operación y administración, gestión de seguridad, etc.

- Los acuerdos de nivel de servicio (ANS) establecidos deben ser monitoreados y revisados regularmente en la etapa contractual para garantizar que se cumple con lo contratado y que se logran los objetivos de disponibilidad de la SSF.

- Se debe considerar lo definido en los Acuerdos Marco Vigentes definidos por Colombia Compra Eficiente, especialmente aquellos asociados a

Servicios de nube pública y Servicios de centro de datos / nube privada, esto teniendo en cuenta los diferentes esquemas del modelo de computación en la nube: Software como servicio (SaaS), Plataforma como servicio (PaaS), Infraestructura como servicio (IaaS).

- El Oficial de Seguridad de la Información debe establecer los esquemas de cifrado necesarios para garantizar la confidencialidad en la sincronización/replicación de la información desde el centro de datos principal hacia el centro de datos de respaldo (en caso de que exista uno). Para esto se deben considerar diferentes esquemas de cifrado:

  - Cifrado individual de archivos o carpetas
  - Cifrado a nivel del sistema de archivos (por ejemplo mediante un sistema EFS)
  - Cifrado de una porción de la información (por ejemplo en el caso de aplicaciones mediante un cifrado a nivel de base de datos)
  - Cifrado en todo el canal de transmisión (por ejemplo mediante una VPN)
  - Cifrado de la conexión hacia ciertas aplicaciones (por ejemplo mediante conexiones https)

- El Oficial de Seguridad de la Información debe liderar el monitoreo regular de la replicación de la información de la SSF hacia el centro de datos contratado, para ello se deben llevar registros de las labores de sincronización y en caso de errores relacionados a la integridad, confidencialidad o disponibilidad de los datos, evaluar la generación de un incidente de seguridad de la información, mediante el procedimiento de gestión de incidentes.

- Los backups realizados sobre la información almacenada en el centro de datos principal/alterno o en una arquitectura de computación en la nube deben estar sujetos a la política PTI020 Respaldo de la Información. Esto implica seguir los lineamientos en cuanto a pruebas sobre los backups realizados y validación de su restauración.

Seguridad de los equipos

3.29. NTI026. Política de Escritorio Limpio y Pantalla Segura.

Políticas Relacionadas: PI009 Escritorio limpio y pantalla limpia.

Objetivo: Incorporar en la SSF, lineamientos de escritorio limpio para documentación física y medios de almacenamiento removibles así como lineamientos de pantalla limpia orientados a los medios de procesamiento de información.

Alcance: Esta norma deberá ser adoptada por todos los colaboradores de la SSF que intervienen dentro del Sistema de Gestión de Seguridad de la Información de la entidad.

Descripción:

Es responsabilidad del Oficial de Seguridad, velar por el cumplimiento de los siguientes lineamientos:

- Cuando la información crítica de la SSF representada en papeles o medios de almacenamiento removibles no está siendo utilizada o la oficina donde se encuentran dichos documentos no es ocupada por personal de confianza, debe guardarse en un recipiente seguro bajo llave como una caja fuerte o un archivador apropiado.

- En los momentos en que el computador no están siendo atendidos por la persona responsable, este equipo debe dejarse apagado o dejar la pantalla bloqueada de manera que solo pueda ingresar dicha persona mediante su clave de acceso.

- Se debe prohibir en uso no autorizado de fotocopias, cámaras digitales, escáner o cualquier mecanismo de reproducción al interior de la SSF.

- No deben permanecer dentro de la impresora los documentos que contienen información confidencial para la SSF.

Seguridad de las operaciones

3.30. NTI027. Política de Gestión de Capacidad.

Políticas Relacionadas: PTI017Gestión de capacidad.

Objetivo: Mediante el monitoreo constante de los recursos de infraestructura, se controle sus capacidades de operación para proyectar con anticipación las posibilidades de operación y disponibilidad confiables para la SSF y asegurar el desempeño futuro de los sistemas.

Alcance: Tiene como cobertura, todos los recursos tecnológicos de la SSF.

Descripción:

- El Coordinador de Servicios Tecnológicos debe, mediante el uso de herramientas de monitoreo y gestión, conocer el comportamiento en tiempo

real de las capacidades de todos los equipos red y servidores que representan la plataforma tecnológica base para el funcionamiento de la SSF.

- Como producto de este monitoreo de capacidades, el Coordinador de Servicios Tecnológicos debe determinar el momento en que se hace necesario realizar un procedimiento de actualización, mantenimiento o cambio de determinado sistema.

- El Coordinador de Servicios Tecnológicos debe entregar al Comité de Seguridad, un reporte trimestral del estado de capacidad de los dispositivos monitoreados indicando el porcentaje de sus capacidades máximas, promedio y mínimas exigidas en periodos de tiempo de un día, una semana y un mes. Esto con el objeto de establecer proyecciones de requerimientos futuros de estos recursos conforme a las exigencias proyectadas de la entidad como por ejemplo, la implementación de nuevos proyectos, el crecimiento de la planta de personal, etc.

Gestión de la Prestación de Servicios de Proveedores

3.31. NTI028. Política de Gestión de Proveedores

Políticas Relacionadas: PA015 Seguimiento y revisión de los servicios de los proveedores.

Objetivo: Definir los mecanismos para realizar un monitoreo y auditoria a los servicios, reportes y registros provistos por los proveedores.

Alcance: Esta norma cubre a los proveedores y terceros que colaboran con la SSF.

Descripción:

- El proceso de gestión de servicios por parte de la SSF a los proveedores y terceros se debe llevar a cabo bajo los siguientes lineamientos a cargo del Oficial de Seguridad con la colaboración del Coordinador de Servicios Tecnológicos y el Responsable de Gestión de Proyectos de Sistemas de Información:

- Se debe monitorear los Acuerdos de Niveles de Servicio (ANS) concertados con cada proveedor o tercero para validar su cumplimiento y tomar medidas correctivas a que haya lugar.

- Se deben revisar los reportes de servicio entregados por los proveedores o terceros para verificar el cumplimiento las actividades desarrolladas y de ser necesario programar reuniones de seguimiento.

- Se debe suministrar la información y elementos necesarios al proveedor o tercero cuando este es requerido para atender un incidente de seguridad conforme esté estipulado en los lineamientos del soporte y los ANSs.

- Se deben hacer seguimientos de auditoria a contratistas y terceros teniendo en cuenta los registros de eventos de seguridad, problemas operacionales, interrupciones de servicio, y demás incidentes relacionados con la manipulación de los contratistas o terceros.

- Se debe dar solución a cualquier incidente detectado en el cual estén involucrados los proveedores o terceros.

- Se deben tomar las acciones correspondientes conforme a las cláusulas de los contratos y los ANSs.

- La SSF en cabeza del Oficial de Seguridad debe siempre mantener el control de todos los sistemas de seguridad de la información que pueden verse afectados por la información confidencial o crítica que las personas contratistas o terceros ingresan, procesan o manejan.

- El Oficial de Seguridad debe establecer una estructura de reportes, formato o proceso que permita hacer trazabilidad o seguimiento a las actividades desarrolladas por los contratistas o terceros.

- Las actividades programadas para ser ejecutadas por un contratista o tercero deben ser validadas por el Oficial de Seguridad con el apoyo del funcionario responsable directo de dicha actividad y someterse al proceso de control de cambios para su aprobación final.

Gestión de activos

3.32. NTI029. Retiro de Activos

Políticas Relacionadas: PTI006 Devolución de activos, PTI003 Inventario de activos, PTI005 Uso aceptable de los activos

Objetivo: Asegurar la confidencialidad, integridad y disponibilidad de los activos de información tipo físico que sean retirados de la Superintendencia del Subsidio familiar.

Alcance: Esta norma define las obligaciones que debe seguir el personal de Superintendencia del Subsidio familiar que retire activos información de tipo físico durante un periodo de tiempo determinado.

Descripción: para retirar los activos de información de la Superintendencia del Subsidio Familiar se debe tener en cuenta los siguientes aspectos:

- Se debe identificar el nombre de los colaboradores con autoridad para realizar el retiro, así como también identificar el nombre de los funcionarios y contratistas que tienen asignados algún activo de información.

- Cualquier activo de información que sea retirado del inventario de activos de la Superintendencia del Subsidio familiar, deberá quedar registrado en el formato de salida temporal de bienes. En este se debe indicar las características y estado del activo, el nombre del colaborador responsable, el tiempo en el cual el activo será reintegrado.

- Los activos de información que sean retirados de las instalaciones de la Superintendencia del Subsidio familiar por ningún motivo deben estar desatendidos en sitios públicos ni en su lugar de permanencia ni durante su traslado.

- Se debe aplicar medidas de seguridad adecuadas que minimicen los riesgos identificados en los entornos físicos que frecuentan los equipos y activos de información (entidades de orden local, comisión nacional (trabajo en campo), trabajo en la residencia del colaborador, etc.), una vez están fuera de las instalaciones de la Superintendencia del Subsidio familiar.

- Los equipos portátiles, tabletas, discos duros e implementos de comunicaciones (cámaras fotográficas, de video, etc.) deberán tener los implementos de seguridad y protección requeridos (maletín, guaya, cargador, espumas, empaque, soportes, candado, etc.), previó a su retiro de las instalaciones.

- Se debe asegurar que los equipos de cómputo que se retiren de la Superintendencia de manera temporal, tengan un inicio de sesión con usuario y contraseña según lo establece la Política de Contraseñas.

Seguridad física y del Entorno

3.33. NTI030. Seguridad física y del entorno

Políticas Relacionadas: PI001 Perímetro de seguridad física, PI002 Controles de Accesos Físicos, PI003 Seguridad de las oficinas, recintos e instalaciones, PI005 Ubicación y protección de los equipos

Objetivo: Definir los aspectos que rodean la seguridad física y del entorno, para disminuir los incidentes asociados a la confidencialidad, integridad y disponibilidad, de los activos de información de la Superintendencia del Subsidio Familiar.

Alcance: Esta norma define los aspectos que debe cumplir las instalaciones de la Superintendencia del Subsidio Familiar para brindar una adecuada seguridad física y del entorno a los activos información.

Descripción: para prevenir el acceso físico no autorizado, el daño y afectación en las áreas que manipulan y resguardan información sensible o confidencial de la Superintendencia del Subsidio Familiar se debe tener en cuenta los siguientes aspectos:

- El perímetro de seguridad debe estar claramente definido en la Superintendencia del Subsidio Familiar especialmente en las áreas que tiene bajo su custodia activos de información sensibles o confidenciales, este perímetro debe hacerse a través de elementos como paredes, puertas de acceso, escritorios de recepción atendidos, etc.

- Se deben instalar mecanismos robustos físicamente (p.ej. cerraduras, alarmas, sistemas lectores de tarjeta, muros, puntos de acceso con vigilancia humana) con el objetivo de prevenir el acceso no autorizado a zonas que contengan activos de información críticos para la Superintendencia del Subsidio Familiar.

- La Superintendencia del Subsidio Familiar debe contar con un sistema de detección de intrusos (sistema de alarmas físico) en sus instalaciones, que debe permanecer activo en horario o laboral y ser sometido a pruebas de manera regular.

- Para el ingreso de visitantes a las instalaciones de la Superintendencia del Subsidio Familiar, el servicio de vigilancia deberá preguntar la oficina destino hacia donde se dirige la persona y el nombre del funcionario que autoriza el ingreso.

- Todos los visitantes deberán ser direccionados por el servicio de vigilancia a la Recepción de las instalaciones, donde se realizará el registro de la persona (nombre, número de identificación, fecha y hora de entrada y nombre del funcionario que autoriza el ingreso), se entregará el mecanismo de identificación de la Superintendencia del Subsidio Familiar el cual se portará en un lugar visible, y se anunciará al funcionario requerido.

- Para los ingresos temporales de visitantes que requieran ingresar a la entidad de manera frecuente, se deberá enviar un comunicado por parte del funcionario responsable que autoriza el ingreso indicando el motivo y duración de la autorización.

- Las puertas y ventanas de las oficinas, salas e instalaciones, que tienen bajo su custodia activos de información de alta criticidad, deben permanecer cerradas con llave cuando no están siendo atendidas. Aquellas oficinas que no tengan puerta, deberán permanecer atendidas mientras se encuentren en ella personal externo a la Superintendencia del Subsidio Familiar.

- Los equipos y dispositivos que son utilizados para soportar las funciones críticas de la entidad, deben estar ubicados en áreas cuyo acceso sea restringido y esté supervisado por los responsables de los mismos.

Cumplimiento de los requisitos legales

3.34. NTI031. Protección de datos personales

Políticas Relacionadas: PA020 Privacidad y protección de información de datos personales

Objetivo: Garantizar la privacidad y la protección de los datos personales de todas las personas que interactúen con la Superintendencia del Subsidio Familiar, para tal fin, se establecerán instrumentos y controles para el adecuado tratamiento de los datos.

Alcance: La Superintendencia del Subsidio Familiar en su calidad de responsable del tratamiento de datos personales, define su alcance para la norma Protección de datos personales teniendo en cuenta la Ley 1581 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales”,

Descripción:

- Es responsabilidad de la Superintendencia del Subsidio Familiar en cumplimiento de su deber legal y reglamentario, hacer efectiva la garantía constitucional de protección a la intimidad personal y familiar de todos los

ciudadanos, estableciendo instrumentos y controles de cara a dar un tratamiento adecuado a la información que administra.

- La entidad asegura la debida reserva de la información personal de las personas o empresas que se encuentran en su base de datos, la cual será utilizada para el envío de información institucional de la entidad.

- La entidad no proporciona la información de sus grupos de interés a ningún tercero, salvo que la persona o empresa lo autorice de forma expresa y por escrito.

- La información obtenida en cualquier registro de datos personales realizado en forma presencial y/o virtual para algún producto o servicio de la Superintendencia del Subsidio Familiar, será utilizada solo para fines institucionales, en ningún momento será compartida ni transferida a terceros para su utilización.

- Las empresas o personas pueden decidir, conocer, actualizar, rectificar y solicitar la eliminación de sus datos personales en cualquier momento a la entidad.

- Para los casos en donde no se puede determinar la voluntad de las personas que comparten sus datos personales con la Superintendencia del Subsidio Familiar, la entidad debe implementar mecanismos de ofuscación de datos sensibles en sus sistemas para evitar la violación de la legislación.

- Todos los contratistas y terceros dentro de la Superintendencia del Subsidio Familiar deben cumplir la cláusula de confidencialidad la información y la cláusula de integridad de la información, definidas en sus contratos. Por otra parte a los funcionarios les aplica el código disciplinario único de la Ley 734 de 2002, en particular el artículo 34 (deberes de todo servidor público) y 48 (faltas gravísimas).

ELABORO		REVISO		APROBO	
Nombre:	Juan José Olivella	**Nombre:**		**Nombre:**	Norberto Agudelo Valencia
Cargo:	Profesional Universitario Oficina de Tecnologías de la Información y las Comunicaciones	**Cargo:**	Profesional Especializado Oficina de Tecnologías de la Información y las Comunicaciones	**Cargo:**	Jefe de Oficina de Tecnologías de la Información y las Comunicaciones
Fecha:	29/Sep./2015	**Fecha:**	29/Sep./2015	**Fecha:**	29/Sep./2015

Línea Gratuita Nacional 018000910110
Calle 45 A No. 9-46
Bogotá Colombia
Fax 3487804
ssf@ssf.gov.co