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



**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**

|  |  |  |
| --- | --- | --- |
|  | **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**

[1. PRESENTACIÓN DEL MANUAL 3](#_Toc434859033)

[1.1. Objetivo de Manual 3](#_Toc434859034)

[1.2. Alcance de las Políticas de Seguridad de la Información 4](#_Toc434859035)

[2. TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN 4](#_Toc434859036)

[3. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 7](#_Toc434859037)

[3.1. Aspectos a tener en cuenta 7](#_Toc434859038)

[3.2. Políticas concernientes a la Administración de la Superintendencia del Subsidio Familiar (PA) 8](#_Toc434859039)

[3.2.1. Políticas de Seguridad de la Información. 8](#_Toc434859040)

[3.2.2. Organización de la Seguridad de la Información - Ref.: ISO/IEC 27001 CL A.6. 9](#_Toc434859041)

[3.2.3. Seguridad de los Recursos Humanos- Ref.: ISO/IEC 27001 CL. A.7 10](#_Toc434859042)

[3.2.4. Gestión de los activos de información- Ref.: ISO/IEC 27001 CL A.8. 12](#_Toc434859043)

[3.2.5. Relaciones con los proveedores - Ref.: ISO/IEC 27001 CL. A.15 13](#_Toc434859044)

[3.2.6. Cumplimiento - Ref.: ISO/IEC 27001 CL. A.18 15](#_Toc434859045)

[3.3. Políticas concernientes a la Oficina TIC de la Superintendencia del Subsidio Familiar (PTI) 20](#_Toc434859046)

[3.3.1. Políticas de Seguridad de la Información - Ref.: ISO/IEC 27001 CL. A.5. 20](#_Toc434859047)

[3.3.2. Gestión de los activos de información- Ref.: ISO/IEC 27001 CL A.8 21](#_Toc434859048)

[3.3.3. Control de accesos- Ref.: ISO/IEC 27001 CL. A.9 23](#_Toc434859049)

[3.3.4. Criptografía - Ref.: ISO/IEC 27001 CL. A. 10 25](#_Toc434859050)

[3.3.5. Seguridad de las operaciones - Ref.: ISO/IEC 27001 CL. A. 12 26](#_Toc434859051)

[3.3.6. Seguridad de las comunicaciones - Ref.: ISO/IEC 27001 CL. A. 13 30](#_Toc434859052)

[3.3.7. Adquisición, desarrollo y mantenimiento de sistemas - Ref.: ISO/IEC 27001 CL. A. 14 34](#_Toc434859053)

[3.3.8. Gestión de incidentes de seguridad de la información - Ref.: ISO/IEC 27001 CL. A.16 38](#_Toc434859054)

[3.3.9. Aspectos de seguridad de la información de la gestión de continuidad del negocio - Ref.: ISO/IEC 27001 CL. A.17 40](#_Toc434859055)

[3.4. Políticas concernientes a Infraestructura (Servicios Administrativos) de la Superintendencia del Subsidio Familiar (PI) 41](#_Toc434859056)

[3.4.1. Seguridad física y del entorno- Ref.: ISO/IEC 27001 CL. A. 11 42](#_Toc434859057)

**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. 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. 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.

1. 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.

1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
	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.
	1. 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.

* + 1. Políticas de Seguridad de la Información.
			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.

* + - 1. 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.

* + 1. 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 y atendiendo a la debida segregación de funciones, se establecen las responsabilidades para las áreas funcionales dentro de la entidad.

* + - 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.
	+ - 1. 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 cual plantea los siguientes aspectos:

* Identificar entidades que representen una figura de autoridad en temas de seguridad de la información.
* Revisar y estudiar 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 de seguridad de la información.
	+ - 1. 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. Por tal motivo, se debeidentificar los grupos de interés especiales de profesionales en seguridad de la información, y será el oficial de seguridad el encargado de la comunicación e interacción con tales grupos de interés.

* + - 1. 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.

* + 1. Seguridad de los Recursos Humanos- Ref.: ISO/IEC 27001 CL. A.7

Es de vital importancia concientizar a los colaboradores 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.

* + - 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 la Superintendencia del Subsidio Familiar debe hacerse responsable de que en el proceso de selección del personal se incluyan criterios que propendan por garantizar la confidencialidad, integridad y disponibilidad de la información a la cual tendrían acceso los futuros colaboradores de la Entidad.

* + - 1. 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 plan anual de divulgación en seguridad de la información 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 la entidad y sus dependencias, 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.

* + - 1. 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:

* Se debe identificar la violación incurrida a las políticas de seguridad de la información de acuerdo al procedimiento de gestión de incidentes de seguridad.
* Cualquier violación a la seguridad de la información (incluidos aspectos de licenciamiento de software y demás) 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 considerará como una posible causal de sanciones acordes a la normatividad vigente.
	+ - 1. 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 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.

* + 1. 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 sobre aquella que le ha sido entregada y que genere un impacto para la SSF.

* + - 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:

* **Ultrasecreta**: Corresponde a aquella Información que al clasificarla en este nivel solo podrá ser accedida por el propietario del activo de información, por lo tanto es el nivel más restrictivo.
* **Confidencial**: Información que por su contenido solo debe ser conocida inicialmente por un grupo reducido de funcionarios y cuya divulgación no autorizada puede ocasionar perjuicios a una determinada área de la entidad o persona.
* **Privada** (Por Defecto): Toda aquella información recibida por parte de la Entidad se asume por defecto como privada, a menos que sea reclasificada por el propietario del activo de información. Esta información se debe proteger del conocimiento de personas extrañas a la Entidad y su divulgación es restringida.
* **Pública**: Es aquella información que por su naturaleza es compartida con la ciudadanía en general, dado que su difusión no representan una amenaza para la SSF o sus colaboradores en términos reputacionales, operativos o legales.
	+ 1. Relaciones con los proveedores - Ref.: ISO/IEC 27001 CL. A.15

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

* + - 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 así asegurar la protección de los activos de la Superintendencia del Subsidio Familiar. Dado lo anterior se establecen los siguientes lineamientos:

* A aquellos 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 no deben tener acceso 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 registrar en la recepción de la Superintendencia del Subsidio Familiar en el momento de su ingreso. Los equipos que ingresan a la SSF y que son necesarios para la realización de la labor del proveedor también deben ser registrados.
	+ - 1. 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 pertinentes con cada proveedor que pueda acceder, procesar, almacenar, comunicar o suministrar componentes de infraestructura de la Oficina de TIC, con el fin de proteger la información de la entidad, teniendo en cuenta los requisitos establecidos en los acuerdos de confidencialidad pactados con el proveedor.

* + - 1. 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.

* + - 1. 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 SSF 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.

* + - 1. 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.

* + 1. Cumplimiento - Ref.: ISO/IEC 27001 CL. A.18
			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 la estrategia de gobierno en Línea se establezcan para la estructuración del SGSI de la entidad.
* Los requisitos legales y regulatorios que afectan la seguridad de la información deben 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.
	+ - 1. 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 establece 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.
* Se deben acatar normas y procedimientos para el cumplimiento de la normatividad vigente.
* La entidad debe difundir las políticas de adquisición de software y las disposiciones de la normatividad vigente.
* Se debe mantener un adecuado registro de activos.
* Se deben conserven pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
* Se debe implementen controles para evitar llegar al número máximo permitido de usuarios.
* Sólo se permite la instalación de productos con licencia y software autorizado.
* Se debe elaborar y divulgar un procedimiento para el mantenimiento en condiciones adecuadas de las licencias.
* Se deben utilizar herramientas de auditoría adecuadas.
* Se deben cumplir los términos y condiciones establecidos para obtener software e información de 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.
	+ - 1. 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.

* + - 1. 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 la entidad, será utilizada solo para fines institucionales, en ningún momento será compartida ni transferida a terceros para su utilización.
	+ - 1. 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.
	+ - 1. 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 de la Información debe velar por el cumplimiento de las políticas, normas y procedimientos de gestión de la información dentro de la Superintendencia del Subsidio Familiar. Así mismo los funcionarios deben aplicar y 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 de la Información debe realizar lo siguiente:

* Establecer las causas del incumplimiento siguiendo el procedimiento de gestión de incidentes.
* 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.
	1. 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.

* + 1. Políticas de Seguridad de la Información - Ref.: ISO/IEC 27001 CL. A.5.
			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 deben tener conocimiento de los riesgos, amenazas y vulnerabilidades de cada activo de información, con el fin de soportar la gestión del riesgo de manera oportuna, garantizando así los principios de confidencialidad, integridad y disponibilidad de la información.

* + - 1. 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 demás controles que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

* + 1. 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 que ha sido entregada para su uso.

* + - 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.

* + - 1. 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 generalmente es el líder del proceso o jefe de área, y quien velará por su buen uso y custodia. El propietario o responsable se encargará de hacer la evaluación de criticidad, definir el nivel de clasificación y ser quien define los requisitos de seguridad del activo.

* + - 1. 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.

* + - 1. 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.

* + - 1. 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 a los equipos de la SSF, 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 estar controlados y físicamente protegidos.

* + 1. Control de accesos- Ref.: ISO/IEC 27001 CL. A.9

Para la entidad debe ser prioritario definir el personal que va a tener acceso a información sensible, por lo cual debe limitar el acceso a las 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. Así mismo es necesario restringir el acceso a las instalaciones donde dicha información se encuentra resguardada, garantizando así la confidencialidad e integridad de la misma.

* + - 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 establece lo siguiente al respecto del acceso a sus recursos computacionales:

* 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 ser permisible únicamente mediante firma impresa y documentación de aceptación de un acuerdo de confidencialidad hacia la entidad, donde el tercero este comprometido con el uso exclusivo del servicio para el que fue provisto el acceso.
	+ - 1. 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 para propósitos institucionales. La Oficina de TIC debe definir los procedimientos para solicitar y aprobar accesos a Internet. Los accesos a contenidos específicos deben ser autorizados formalmente por el Jefe inmediato del personal que solicita el acceso, y se debe contar con la viabilidad por parte de la Oficina TIC quien considerará los impactos a nivel de seguridad que el acceso puede generar. Asimismo, la Oficina TIC debe definir las pautas de utilización de Internet para todos los usuarios.

* + - 1. 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 una red inalámbrica de la SSF, los funcionarios, contratistas y demás personal deben:

* Conectarse a las redes inalámbricas a través de un esquema de autenticación y autorización aprobado por la Oficina TIC.
* Acceder a la red inalámbrica de la entidad siguiendo un proceso de identificación de las direcciones MAC de los dispositivos.
	+ - 1. 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 debe seguir un proceso formal de creación, modificación o cancelación de cuentas de usuarios, con el propósito de permitir la administración de los derechos de acceso.

* + - 1. 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 las normas, procesos, procedimientos y guías pertinentes.

* + 1. 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 debe utilizar sistemas y técnicas criptográficas para la protección de la información.

* + - 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:**

Se deben implementar mecanismos de protección de información que cumplan con la reglamentación, políticas y estándares aplicables en la legislación colombiana. Igualmente se presentan los siguientes lineamientos:

* Se debe proporcionar una protección adecuada a los equipos utilizados para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
* Se debe proteger las claves secretas y privadas evitando que sean copiadas o modificadas sin autorización.
	+ - 1. PTI014. Título de la Política: Gestión de Claves - 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, envíen y reciban información fidedigna, verás e integra.

* + 1. Seguridad de las operaciones - Ref.: ISO/IEC 27001 CL. A. 12

Se debe proteger 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.

* + - 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 y asegurando la disponibilidad de la información.

* + - 1. PTI016. Título de la Política: Gestión de cambios - Ref.: ISO/IEC 27001 CL. A. 12.1.2

**Definición de la Política:**

Se debe implementar y mantener una gestión de cambios en la entidad, especialmente en aquellos procesos de negocio, instalaciones y 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 de la Información y las partes interesadas en la entidad.

* + - 1. 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 de capacidad de almacenamiento de información, comprometiendo la disponibilidad de la misma. Además se deben tener en cuenta las siguientes medidas:

* Implementar 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.
* En caso de que no exista un sistema de monitoreo de capacidad centralizado o que por la naturaleza del dispositivo este no pueda integrarse a dicho sistema, es el responsable de cada dispositivo quien deberá realizar el monitoreo permanente de la capacidad del mismo.
	+ - 1. PTI018. Título de la Política: Separación de los ambientes de desarrollo, pruebas y producción. - 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 SSF 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 la plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar la operación. Por lo anterior se deben tomar en consideración los siguientes factores:

* El paso de software y hardware de un ambiente a otro se debe controlar y gestionar.
* Los usuarios deben contar únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.
* No se deben realizar pruebas, instalaciones o desarrollos directamente sobre un entorno de producción. Esto con el fin de evitar problemas de disponibilidad o confidencialidad de la información.
* El ambiente del sistema de prueba debe emular el ambiente de producción lo más estrechamente posible.
* No se debe permitir la copia de información Ultrasecreta o Confidencial de la entidad, desde el ambiente de producción al ambiente de pruebas; en caso de que sea estrictamente necesario, la copia la debe autorizar el propietario de la información y el Oficial de Seguridad de la Información y se deben implementar controles que garanticen la confidencialidad de la información y esta se elimine de forma segura después de su uso.
* Se debe restringir el acceso a 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 deben verificar las versiones instaladas de software tanto en el ambiente de pruebas como en el de producción y se debe confrontan esta información con revisiones previas.
* Se deben establecer roles y responsabilidades en cada fase del desarrollo o modificación de los sistemas de información de la entidad.
	+ - 1. 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 están protegidos contra códigos maliciosos se deben implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia para la protección de los usuarios contra códigos maliciosos.

* + - 1. 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 la información 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 en función de su criticidad, y ponerlas a prueba regularmente con el fin de asegurar la integridad y disponibilidad de la información.

* + - 1. 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 de los usuarios, excepciones, fallas y eventos de seguridad de la información, que se encuentran relacionados a activos de información críticos para la SSF.

* + - 1. 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 TIC en conjunto con el Oficial de Seguridad de la Información y los propietarios de los riesgos asociados a los activos de información deben establecer los criterios necesarios que permitan el aseguramiento de la información de registro, basados en el nivel de criticidad de cada activo de la entidad. Por tal fin, las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

* + - 1. 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 y confidencialidad de la información debe existir un registro de cualquier modificación realizada por el administrador de los sistemas de procesamiento de 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.
	+ - 1. 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; evaluar la exposición de la entidad a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

* + - 1. 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 la necesidad de la instalación del nuevo software. Cuando sea autorizado por el jefe inmediato, este 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.

* + 1. **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 deben establecer ciertos parámetros que garanticen la confidencialidad e integridad de la información transmitida.

* + - 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.

* + - 1. 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. Adicionalmente, con el fin de garantizar la confidencialidad e integridad de la información se deben establecer las siguientes medidas:

* Se deben mantener instalados y habilitados sólo aquellos programas, aplicativos o servicios que sean utilizados por los colaboradores de la entidad o demás personas autorizadas para su manejo.
* Se debe controlar el acceso lógico a los programas, aplicativos o servicios a los cuales tienen acceso los usuarios.
* Se debe configurar cada programa, aplicativo o servicio de manera segura, evitando que queden expuestas las vulnerabilidades que se pudieran generar.
* Se deben instalar y verificar periódicamente las actualizaciones de seguridad realizadas.
	+ - 1. 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.

* + - 1. 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, etc.) para el envío o recepción de cualquier tipo de información relacionada con la entidad.
* Está prohibido el uso de mecanismos de transferencia o almacenamiento de información basados en la nube que no sean autorizados por la Oficina TIC y para los cuales no se tenga contratado un servicio corporativo que garantice la confidencialidad de la información transferida a la nube.
* 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.
	+ - 1. 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 formales para proteger la transferencia de información a través todo tipo de sistema 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 transferida entre la entidad y los usuarios de la página web, debe tener la seguridad necesaria para el 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 Ultrasecreta se deben establecer acuerdos de confidencialidad.
	+ - 1. 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. De esta forma se establecen los siguientes lineamientos:

* 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 a la mesa de ayuda, para evitar que un posible malware pueda afectar 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 puede ser motivo de suspensión temporal de la cuenta de correo e incluso de una posible falta disciplinaria, y en cualquier caso el evento debe ser atendido por el procedimiento de gestión de incidentes de seguridad, conforme al impacto causado a la seguridad de la información.
* La Oficina TIC se reserva el derecho de monitorear el servicio de correo electrónico ante eventos sospechosos que comprometan la seguridad de la información de la Entidad.
	+ - 1. 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 o terceros, se les incluirá dentro de los contratos con la SSF, cláusulas de confidencialidad y reserva de la información a la cual tengan acceso mientras permanezcan en la entidad.
	+ 1. 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:

* + - 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 del software. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

* + - 1. 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 debe establecer los requisitos relacionados con seguridad de la información para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

* + - 1. 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 TIC debe protegerse contra actividades fraudulentas, disputas contractuales y eventos de divulgación y modificación no autorizada de la información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas.

* + - 1. 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 TIC.

* + - 1. 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.

* + - 1. 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 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 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. Para esto se requiere de un comité de gestión de cambios integrado a la estructura actual de la Oficina TIC.
* Los cambios técnicos en los sistemas de información o en la plataforma tecnológica deben ser documentados por la Oficina TIC.
* Todo cambio que se realice en los sistemas de información o en la plataforma debe ser 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.
	+ - 1. 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 TIC debe revisar las aplicaciones críticas del negocio relacionadas al cambio, 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 y ejecutados por la Oficina TIC.

* + - 1. 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 deben ser autorizados, supervisados y realizados por funcionarios de 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 Oficina TIC, 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.

* + - 1. 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 restringir las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente siguiendo el procedimiento de gestión de cambios, 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.

* + - 1. 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 las actividades de desarrollo, pruebas, aseguramiento de la calidad y paso a producción de los desarrollos hechos por los contratistas.

* El nuevo software debe garantizar la confidencialidad, integridad y disponibilidad de los demás sistemas de información, aplicaciones, programas con los que ya 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.
	+ - 1. 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 de 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 la plataforma donde operara de forma permanente: 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 de forma concurrente 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 el aplicativo y validar su estabilidad.
	+ 1. Gestión de incidentes de seguridad de la información - Ref.: ISO/IEC 27001 CL. A.16

La entidad debe gestionar los incidentes de seguridad de forma eficaz y eficiente, de tal forma que se disminuya el impacto que estos pudieran generar a la entidad.

* + - 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 de la Estrategia de Gobierno en Línea (GEL) “La entidad debe implementar una capacidad para el manejo de incidentes, de manera que incluya: preparación, detección, análisis, contención, erradicación y recuperación”.

* + - 1. **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 de la Información o a las autoridades de seguridad de la información establecidos en la entidad.

* + - 1. 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 establecer mediante un procedimiento de gestión de incidentes los criterios que utilizará para la evaluación de los eventos de seguridad que se presenten, y de esta forma determinar cuáles de ellos corresponden a un incidente de seguridad y deben ser tratados como tal.

* + - 1. 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, con el fin de que sean evaluados como posibles soluciones para incidentes futuros en la entidad.

* + - 1. 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 en situaciones en las que se presente un incidente de seguridad.

* + 1. Aspectos de seguridad de la información de la gestión de continuidad del negocio - Ref.: ISO/IEC 27001 CL. A.17

La entidad debe implementar 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.

* + - 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.

* + - 1. 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.

* + - 1. 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.

* + - 1. 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 de los servicios tecnológicos ofrecidos por la Oficina TIC.

* 1. 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.

* + 1. Seguridad física y del entorno- Ref.: ISO/IEC 27001 CL. A. 11

La seguridad física y del entorno 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.

* + - 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 para proteger áreas que contengan información confidencial o ultra secreta, al igual que instalaciones para el manejo de información.

* + - 1. PI002. Título de la Política: Controles de Acceso 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 Información de la Superintendencia del Subsidio Familiar y la Oficina TIC, con la finalidad de permitir el acceso sólo al personal autorizado.

* + - 1. 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 Confidencial o Ultrasecreta, las cuales deben ser protegidas 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.
* Las disposiciones y normas (estándares) en materia de sanidad y seguridad vigentes. Asimismo, se considerarán las amenazas que representan los edificios y zonas aledañas.
	+ - 1. 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.

* + - 1. 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, garantizando el acceso únicamente al personal autorizado para su uso teniendo en cuenta los siguientes aspectos:

* Se deben ubicar los equipos en zonas de la entidad donde se minimice el acceso por pate de personal no autorizado.
* Se deben ubicar las instalaciones de procesamiento y almacenamiento de información que contienen información confidencial o Ultrasecreta, en una zona que permita la supervisión durante su uso.
	+ - 1. 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.

* + - 1. 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.

* + - 1. 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 TIC debe mantener un control actualizado de la frecuencia de realización del mantenimiento preventivo de los equipos en la entidad.

* + - 1. 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 escritorio limpia para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantalla limpia 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 |
| **Fecha:** | 9/Nov/2015 | **Fecha:** | 9/Nov/2015 | **Fecha:** | 9/Nov/2015 |