



INFORME DE SISTEMA DE GESTIÓN DE SEGURIDAD DE

SISTEMAS DE INFORMACIÓN (SGSI).

PROYECTO:

SISTEMA DE GESTIÓN Y

CONTROL DE ASISTENCIA DE APRENDICES

RAZÓN SOCIAL:

SENASISTENCIA

INSTITUCION:

SERVICIO NACIONAL DE APRENDIZAJE

SENA

2017

**Índice**

[**1. Introducción:**](#_30j0zll)3

[1.1. Alcance:](#_1fob9te) 3

[**2. Términos y definiciones**](#_3znysh7)4

[2.1. Seguridad de la información](#_2et92p0) 4

[2.4. Comité de seguridad de la información](#_tyjcwt) 6

[2.5. Responsable de la seguridad informática](#_3dy6vkm) 6

[2.6. Incidente de seguridad](#_1t3h5sf) 6

[**3. Política de seguridad en la información**](#_4d34og8)7

[Politica](#_2s8eyo1) 9

[3.1. Aspectos generales](#_17dp8vu) 9

[**4. Organización de la seguridad Generalidades**](#_3rdcrjn)10

[4.1 Comité de seguridad de la información](#_26in1rg) 11

[**5. Clasificación y control de archivos**](#_lnxbz9)13

[5.1. Inventario de archivos](#_1ksv4uv) 14

# **1.** **Introducción:**

En el informe de sistema de gestión de la seguridad de la información, se evidencia las políticas y protocolos de tratamiento de datos del proyecto SENASISTENCIA; tanto en aspectos legales como responsabilidades del usuario, evaluación y mitigación de riesgos, protocolos de seguridad, normativa y sanciones por el mal manejo de seguridad en la información, lineamientos de proceso de notificación de errores. También se tratarán aspectos como políticas de privacidad y condiciones de uso.

Para generar una normativa adecuada para nuestro proyecto hemos decidido basarnos en el estándar propuesto por la **ISO/IRAM 17799** como modelo para la gestión de la seguridad de la información y la norma **ISO/IEC 27001** que establece el estándar para la creación de un **SGSI**; complementario a esto optamos por apegarnos a la normativa dictada por el Gobierno Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones en la ley estatutaria **1581 de 2012** - Por la cual se dictan disposiciones generales para la protección de datos personales y la ley **1341 de 2009** -Por la cual se dictan disposiciones generales para tecnologías de la Información y aplicación de seguridad.

## **1.1.** **Alcance:**

En el presente informe de sistema de gestión de la seguridad de la información establece las pautas a seguir para tener un buen manejo de la seguridad de la información en los procesos que maneja la empresa, además dicta también sanciones y protocolos a seguir en momentos de ataques maliciosos, copias de seguridad, funciones del área de seguridad informática de la empresa.

este informe debe ser conocido por todo el personal; aunque este no esté directamente relacionado con el área de seguridad informática de la empresa, además también cuenta con un apartado dirigido explícitamente al cliente, aquí se estipulan sanciones por el mal uso o manejo de la información por parte del cliente, políticas de privacidad y condiciones de uso.

**Nota:** la empresa habilitará públicamente y enfocado al cliente estas políticas; en especial aquellas que lo afecten directamente, **el cliente** deberá leer en su totalidad y aceptar las **políticas de privacidad y condiciones de uso**; estas dictaran el tratamiento que se le darán a sus datos y todos los reglamentos para promover las buenas prácticas de seguridad; la empresa **NO SÉ HARÁ RESPONSABLE** por el mal uso de la información que pueda darle el cliente.

# **2. Términos y definiciones**

Para mejor entendimiento de algún asunto y reglas se aplican las siguientes definiciones:

## **2.1. Seguridad de la información**

La seguridad de la información se conoce como medidas preventivas de la siguiente característica:

* **Confidencialidad**: únicamente se dará la información a las personas autorizadas a tener acceso a la misma.
* **Integridad**: se protegerá con exactitud y totalidad de la información, los métodos de procesamiento a cualquier modificación solo autorizada.
* **Disponibilidad:** se garantiza a todos los usuarios autorizados tengan el acceso a la información y recurso relacionados con la misma, en el momento que se requieran para que funcionen correctamente.
* **Autenticidad:** se garantizará el origen o generador de la información, solo se validará al emisor de la información evitando suplantación de identidades.

Adicionalmente se considerará las siguientes definiciones:

* **Auditabilidad:** permite registrar y vigilar la utilización de los recursos a los usuarios autorizados para su posterior control.
* **No repudio:** se evitará que una entidad interrumpa o se haga acreedor de la información que se envíe o reciba donde se alegue ante terceros de lo anterior procedido.
* **Protección a la duplicación**: este evitara que entidades no autorizadas a la información repliquen dicha información, esta transacción solo se realizará una vez, a menos se especifique lo contrario logrando asegurar los datos, proteger la información y facilitar la gestión de equipos involucrados, en sí no haya clonación de la información.
* **Legalidad:** referido a las leyes, normas, reglamentos o disposiciones al as que estén sujetas dicha empresa.
* **Confiabilidad de la Información:** se refiere, cada vez que la información que se genera sea la adecuada para sustentar la toma de decisiones, ejecución de cada labor y funciones requeridas por los usuarios.

Para un mejor entendimiento de la presente Política, se realizan las siguientes

Definiciones:

* **Información:** se refiere a toda comunicación o representación de datos organizados y convenientemente procesados que nos permite extraer cada uno de los conocimientos para la toma de decisiones, para el seguimiento eficaces de los **objetivos** propuestos mediante una actuación adecuada.
* **Sistema de Información**: se refiere a **componentes** (personas, datos, actividades o recursos naturales, etc.) que interaccionan entre sí para alcanzar una meta o fin determinado, para satisfacer las necesidades de la información de dicha organización, apoyando la toma de decisiones y controlar lo que ocurre en la **organización**.
* **Tecnología de la Información:** se refiere al software y hardware operados por el la empresa u Organización, para procesar la información, llevando funciones propias de la Organización (transmisión, procesamiento y almacenamiento de datos), sin importar qué tecnología se utilice.
* **Superusuario:** se refiere al desarrollador de la empresa, se encargará de ingresar toda la información a la base de datos y será el único que podrá crear, modificar, consultar y eliminar(inactivar) cada vez que el cliente lo requiera, para el buen funcionamiento de la empresa.
* **Administrador:** se refiere a los coordinadores de la empresa(SENA), son los encargados de crear la información y monitorear los centros de formación, las sedes, los ambientes de formación, los programas de formación y a los aprendices(cambiar el estado de inasistencia y subir las justificaciones, cambiar el estado de inactivo a activo o viceversa, cambiarlo de suspendido o retirado y tendrá la opción de crear usuario activarlos e inactivar los del sistema)

* **Usuario:** se refiere a los instructores, serán los encargados de registrar las asistencias de los aprendices, habrá seguimiento de reportes como compromisos, advertencias por incumplimiento del reglamento del SENA, revisar novedades de la ficha como la deserción, cargar excusas de los aprendices, generar reportes actualizados de la ficha.

**2.2. Evaluación de riesgos**

La evaluación de riesgos consiste en identificar la vulnerabilidad y posibles amenazas a las cuales se encuentran expuestas la información, logrando evaluar su probabilidad de ocurrencia y el impacto que se generará, funcionando en dicha Organización.

**2.3. Administración de riesgos**

Se entiende como administración de riesgos a un método sistemático que sirve para identificar y administrar los riesgos de la organización, logrando alinear los riesgos y los objetivos de la seguridad, utilizando los recursos de una manera eficiente, reduciendo costos e imprevistos, con mejoras a la capacidad de respuesta a los riesgos. Debe ser cíclico y periódico para su buen uso.

## **2.4. Comité de seguridad de la información**

El comité de seguridad de la información, son un ente directivo integrado por representantes de distintas áreas de la Organización, garantizarán de forma organizada y puntual el apoyo a las autoridades a las iniciativas de la seguridad de la Organización.

## **2.5. Responsable de la seguridad informática**

El responsable de la seguridad informática es aquella persona que cumpla una buena función de supervisar y asesorar el cumplimiento de las políticas de seguridad planteadas cuando se requiera y se necesite a cada uno de los integrantes de esta organización.

## **2.6. Incidente de seguridad**

Un incidente de seguridad es un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de la información que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad, un intento o amenaza de la organización al tratar de destruir su mecanismo de seguridad

# **3. Política de seguridad en la información**

**Generalidades**

Dependemos de la información para que nuestra empresa funcione, sin ella, el pilar central de nuestra compañía y de nuestro proyecto se derrumbaría, debido a que la información es nuestro recurso principal o “materia prima” hemos dedicado mucho de nuestro tiempo para darle el mejor uso y protegerla de diversas amenazas.

Es relevante que se usen los mejores estándares de seguridad al alcance de nuestra empresa, los sistemas de información y en especial todas las cosas relacionadas con Internet están en constante cambio, por eso hemos de garantizar que en la medida de lo posible haremos todo lo que esté al alcance para gestionar procesos de seguridad en nuestra empresa.

No obstante, se sabe que ningún sistema informático, en especial aquellos que están abiertos al mundo por medio de Internet pueden ser 100% seguros, por tanto, este informe promueve las buenas prácticas de seguridad para la mitigación de riesgos posibles.

**Objetivo**

Establecer los lineamientos a seguir para la prevención, mitigación y confrontación de amenazas a la seguridad de nuestra información, ya sea por factores externos, internos o accidentes hemos establecido una política y protocolos a seguir para dichas circunstancias.

**Alcance**

Estas políticas aplican a todo el personal de la empresa, estén directamente relacionados con el área de seguridad informática o no.

**Responsabilidades**

Todas las personas que cuenten con manipulación del **Software o Hardware** de la empresa **están en la obligación de conocer y aplicar esta política de seguridad,** de no acatarse dicha regla la responsabilidad recae en la persona que incumplió y en sus superiores.

Esta política debe ser transmitida en su totalidad a todo el personal o ente participante en la empresa, por medio de los directores de cada área de la empresa.

El **Comité de seguridad informática,** establecerá los lineamientos y políticas a seguir basados en los estándares de seguridad propuestos por la comunidad informática, también será encargado de facilitar la información al personal y demás entes participantes de los procesos de la empresa, deberán diseñar e implementar políticas de seguridad y deberán contar con planes de contingencia para momentos críticos donde la seguridad de la información se vea afectada.

Brindaran soporte tanto al cliente como a la misma empresa en cuanto a seguridad informática se refiere, tener conocimiento y control de las posibles amenazas tanto internas como externas.

El **Propietarios de la información** refiriéndonos a un aspecto técnico dentro de la empresa y no a un ámbito jurídico como el cliente; serán responsables de mantener actualizada la información y de asignar los distintos permisos a la información mediante usuarios clasificados anteriormente.

El **Responsable del Área de Recursos Humanos** o quien desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continúan en materia de seguridad.

Los **Usuarios (clientes) del sistema** serán responsables de conocer en su totalidad la política de seguridad, políticas de privacidad y condiciones de uso y tiene el deber de facilitar información verídica, real y concreta; estará en la obligación de dar un buen uso de la información con la que él cuenta.

El **Área Informática** cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la empresa. Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

## **Política**

## **3.1. Aspectos generales**

La siguiente política se compone de una serie de normas sobre aspectos específicos de seguridad de la información:

* **Organización de la información:** la gerencia del comité de seguridad informática será el área de más rango en cuanto a control y seguridad de la información de la empresa, deberá encargarse de divulgar al personal todos los aspectos de este informe; cada incidente de seguridad debe ser documentado y según su complejidad escalado a sus superiores hasta ser el comité de seguridad la última instancia a encargarse del acontecimiento.
* **Clasificación y control de archivos:** en cuanto a la gestión de proyectos en conjunto utilizaremos la herramienta on-line **Trello** como sistema de integración continua; lo que nos permitirá llevar control de las tareas y su proceso, en cuanto al código de los proyectos manejaremos el sistema de control de versiones **Git;** se manejarán copias de seguridad semanales.
* **Seguridad del personal:** sé implementara una capacitación a todo el personal sobre hábitos para obtener buena higiene de seguridad en la información que maneje cada empleado.
* **Gestión de las comunicaciones y las operaciones:** todos los días se hará una pequeña reunión de máximo 30 minutos, donde cada líder de área preguntará al personal bajo su cargo sobre avances, novedades o cambios sobre el proyecto en concreto que maneje el líder; cualquier acontecimiento deberá ser notificado al supervisor de área y copiado a toda área que resulte afectada por dicho acontecimiento.
* **Desarrollo y mantenimiento de los sistemas:** sé debe garantizar el control y la protección de la información que se maneje durante toda la vida útil del producto, desde el momento de la recolección de datos hasta la implementación del software o actualizaciones posteriores.
* **Administración de la continuidad de las actividades:** el proceso de almacenamiento de la información es un servicio tercerizado por compañías dedicadas a dicha tarea, no obstante, también se manejan copias de seguridad locales de la información más importante de cada proyecto.

* **Cumplimiento:** cada líder de proyecto establecerá fechas límite “relativas”, debido a que debemos contar con supuestos contratiempos que puedan presentarse a lo largo del proyecto; el personal debe hacer todo lo posible por cumplir con las fechas de entrega de presentarse contratiempos el empleado deberá notificar a su superior a cargo.

**3.2. Sanciones previstas por incumplimiento**

Se sancionará administrativamente a todo aquel que incumpla con los debidos procesos de la empresa, dependiendo del rango de importancia de la falta o la magnitud será o no causal de despido, el caso deberá ser informado por el superior de la persona faltante, y el consejo evaluará la sanción a imponer.

# **4. Organización de la seguridad Generalidades**

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la empresa.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Por otro lado, debe tenerse en cuenta que ciertas actividades de la empresa pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

**Alcance**

Esta Política se aplica a todos los recursos del y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

**Responsabilidad**

El Coordinador del Comité de Seguridad de la Información será el responsable de impulsar la implementación de la presente Política.

El Comité de Seguridad de la Información tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la máxima autoridad de la empresa, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.

El Responsable de Seguridad Informática asistirá al personal de la empresa en materia de seguridad de la información y coordinará la interacción con entidades especializadas. Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos a la información y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma. Los Responsables de las Unidades Organizativas cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

El Responsable del Área de Administración cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

## **4.1 Comité de seguridad de la información**

La seguridad de la información es una responsabilidad de todos aquellos que están en contacto con ella, por lo cual se crea el **comité de seguridad de la información**, que está conformado por un número impar de integrantes, de esta forma no habrá decisiones que queden divididas por igual.

Conformación del comité de seguridad de la información

|  |  |
| --- | --- |
| **Área de la empresa** | **Representante** |
| Diseño y Desarrollo | David Rugeles Cano |
| Backend | Luis Forero Torres |
| Documentación | Jeame Suarez Useche |
| Requerimientos y pruebas | Johanna Forero Gonzalez |
| Recursos humanos | Laura Tovar Lopez |

Este Comité tendrá entre sus funciones:

* Revisar y proponer la Política y las funciones generales en materia de seguridad de la información.
* Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
* Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
* Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
* Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
* Garantizar que la seguridad sea parte del proceso de planificación de la información.
* Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
* Promover la difusión y apoyo a la seguridad de la información dentro de la empresa.

# **5. Clasificación y control de archivos**

**Generalidades**

La empresa debe tener total conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

* Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
* Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, etc.
* Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado).
* Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información. Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para la empresa.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos. La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel.

Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información. Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

**Objetivo**

Garantizar que los activos de información reciban un apropiado nivel de protección.

Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

**Alcance**

Esta Política se aplica a toda la información administrada en la empresa, cualquiera sea el soporte en que se encuentre.

## **5.1. Inventario de archivos**

Se identificarán los archivos importantes asociados a cada departamento o sistema, se buscarán sus respectivos propietarios y su ubicación, para luego realizar un inventario de dicha información. El encargado la gestión de documentos deberá hacer un control trimestral de los archivos, verificar su estado y utilidad también deberá mantener dichos archivos actualizados.