No. Versión	Fecha Versión	Descripción del Cambio
00	01/12/2019	Versión Inicial

Fecha de emisión original:	Número de Versión:	Motivo de la Emisión:	Fecha de Emisión:
01/12/2019	00	Creación del Documento	01/12/2019
Elaboró:	**Revisó:**	**Revisó:**	**Aprobó:**
ISC. Roberto Alejandro Mota Diaz **Gerente de Sistemas y Ciber Seguridad**	NA	NA	ING. Pedro Enrique Rivera Ruiz **Director General**

Tabla de contenido

1. PROPÓSITO

Esta política se establece para:

- Informar a los usuarios de Grupo SUSESS: directivos, empleados, contratistas y otros usuarios autorizados de los requerimientos obligatorios para proteger los activos de información y tecnología de la compañía,
- Definir en Grupo SUSESS un enfoque o marco de referencia general para la seguridad de la información basado en las mejores prácticas internacionales y en estándares como ISO 27001:2013,
- Describir los activos de información y tecnología que deben ser protegidos e identificar las amenazas para esos activos,
- Proteger la reputación de Grupo SUSESS con respecto a sus responsabilidades legales y éticas,
- Observar los derechos de los clientes respecto a la información que es de su propiedad y que por motivos de negocios comparten con Grupo SUSESS.

2. ALCANCE

Esta política aplica a cada uno y todos de los siguientes:

1. Dirección, socios y accionistas de Grupo SUSESS.
2. El personal, becarios, proveedores de bienes y servicios y otros usuarios autorizados de Información Institucional y de recursos de TI.
3. Todo el uso de Información Institucional, independientemente de su ubicación (física o en la nube) propiedad de cualquier cuenta de negocios o dispositivo que se use para almacenar, acceder, procesar, transmitir o controlar la información institucional.
4. Los dispositivos de hardware, independientemente de su ubicación o propiedad, cuando están conectados a una red de Grupo SUSESS o a un servicio en la nube para almacenar o procesar información institucional.
5. Los dispositivos de comunicaciones tanto para acceso a la red de área local como para acceso a internet incluyendo ruteadores, tablas de enrutamiento, hubs, multiplexores, modems, switches, firewalls, líneas privadas y herramientas y software de administración de redes.
6. El software de sistemas incluyendo: sistemas operativos, sistemas de administración de bases de datos, sistemas de respaldo y recuperación de datos, protocolos de comunicaciones, entre otros.
7. El software de desarrollo incluyendo: entornos de desarrollo integrales (IDE), editores de texto, compiladores, software de control de versiones, software de administración de dependencias, entre otros.

8. El software de aplicación: usado por los distintos departamentos de la compañía, incluyendo licencias comerciales adquiridas y aplicaciones desarrolladas internamente.
9. El código fuente de los desarrollos de aplicaciones en general y del Control Volumétrico regulado por el Anexo 30 de la Resolución Miscelánea Fiscal de 2019, en particular, incluyendo modelo y diccionario de datos, diagrama de flujo de datos y diagrama de implementación.

Cada empleado debe adherirse a esta política, así como a sus directrices y procedimientos. Los empleados que no cumplan con estas directivas serán sujetos de acciones disciplinarias.

3. OBJETIVO

Esta política se establece con el objetivo de incorporar prácticas de seguridad de la información que permitan asegurar la Confidencialidad, la Integridad y la Disponibilidad de la información institucional de Grupo SUSESS para que a través de ello podamos garantizar que la información es Completa, de Calidad y Útil para el trabajo de los miembros de la organización.

Para lograr este objetivo la Dirección toma la responsabilidad de implantar, mantener y mejorar de manera continua un Sistema de Gestión de Seguridad de la Información (SGSI) con base en las mejores prácticas aceptadas internacionalmente que permita lograr niveles adecuados de seguridad para los activos de información institucionales que sean relevantes, para así garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de manera documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios que se presenten en los riesgos, la tecnología y el entorno.

Cada proveedor debe adherirse a esta política, así como a sus directrices y procedimientos. Los proveedores que no cumplan con estas directivas serán sujetos de acciones disciplinarias, el incumplimiento de esta política por parte de un proveedor puede ser causal de rescisión de contrato.

4. IDENTIFICACIÓN DE AMENAZAS

Se identifican como principales amenazas a la seguridad de la información:

4.1. EMPLEADOS

Los empleados pueden llegar a dañar los sistemas ya sea por falta de capacitación o por dolo. Para mitigar esta amenaza se establece lo siguiente:

- Solo se deben proporcionar los derechos apropiados a los sistemas que correspondan a los roles del empleado.
- Se limita el acceso solo a horas laborales.
- Está prohibida la compartición de cuentas de usuario.
- Durante periodos disciplinarios, no laborables o de separación se deben remover o limitar los accesos a los sistemas según corresponda.
- Se deben llevar y mantener registros de actividad y uso de los recursos TI.
- Los activos de TI deberán contar con control de acceso físico, de tal forma que solo el personal autorizado pueda acceder a ellos.
- Se firmará un contrato de confidencialidad.

4.2. HACKERS AFICIONADOS O AMATEURS

Este tipo de personas son los atacantes más activos en Internet. La probabilidad de ataque de esta fuente es alta. Este tipo de ataques caen en la categoría de crímenes de oportunidad. Los atacantes amateurs normalmente barren Internet en busca de fallas de seguridad públicamente conocidas en la comunidad hacker que no hayan sido atendidas por las organizaciones. Los servidores web y de correo electrónicos son sus blancos preferidos. Una vez que encuentran una vulnerabilidad la atacan normalmente plantando virus o caballos de Troya informáticos o usando los recursos de la organización para sus propios fines. Cuando no encuentran una debilidad fácil de atacar suelen desistir y buscar otro objetivo.

4.3. SABOTEADORES Y HACKERS CRIMININALES

La probabilidad de este tipo de ataque es baja, pero dado la cantidad de información sensible en las bases de datos no es imposible que se llegue a dar. Las habilidades de este tipo de atacantes son de un nivel medio a alto y es posible que tengan entrenamiento relacionado con las herramientas más novedosas de hackeo. Sus ataques están bien planificados y se basan principalmente en debilidades previamente descubiertas en las redes de comunicación.

4.4. PROVEEDORES Y PRESTADORES DE SERVICIOS

Al igual que los empleados, pueden llegar a dañar los sistemas ya sea por falta de capacitación o por dolo. Para mitigar esta amenaza se establece lo siguiente:

- A cualquier proveedor solo se le puede dar acceso a los activos de información cuando sea estrictamente necesario a causa de la actividad que vaya a realizar y posterior a la firma de un acuerdo de confidencialidad.
- Solo se deben proporcionar los derechos apropiados a los sistemas que correspondan al servicio a prestar.

- Se limita el acceso solo a horas laborales.
- A cada individuo que sea parte del proveedor se le debe proporcionar una cuenta individual de usuario.
- Se deben llevar y mantener registros de actividad y uso de los recursos TI.
- Los proveedores también deberán pasar por el control de acceso físico a los recursos de TI.
- Se firmará un contrato de confidencialidad.

4.5. CONFIGURACIONES AMBIENTALES

Representan la principal amenaza a la disponibilidad de la información. Dentro de las contingencias que pueden afectar la disponibilidad de la información de Grupo SUSESS se encuentran, por la localización geográfica de sus instalaciones, los huracanes y las inundaciones. Para mitigar su impacto se debe establecer un Plan de Continuidad del Negocio, el cual debe probarse y mantenerse actualizado.

4.6. DESASTRES AMBIENTALES Y SINIESTROS

Al igual que las contingencias ambientales son una amenaza a la disponibilidad de la información. Además de los huracanes y las inundaciones se deben considerar siniestros como los incendios. En cuanto a los fenómenos naturales se debe tomar en cuenta la posibilidad de que su fuerza sea de tal magnitud que lleguen a dañar seriamente las instalaciones. Para mitigar su impacto se debe establecer además del Plan de Continuidad del Negocio mencionado en el inciso anterior, un Plan de Recuperación de Desastres, el cual también debe mantenerse actualizado.

5. DEFINICIONES

Para una más fácil consulta, estos son los términos empleados en esta política:

INFORMACIÓN: es la interpretación que se le da a un conjunto de datos organizados y procesados que constituyen un mensaje que es capaz de cambiar el estado de conocimiento del sujeto o sistema que lo recibe. Puede residir en papel o en medios electrónicos.

INFORMACIÓN INSTITUCIONAL: Término amplio que describe todos los datos e información creados, recibidos y/o recolectados por Grupo SUSESS.

INFORMACIÓN CONFIDENCIAL: es aquella que cuyo acceso está restringido a un grupo de usuarios o personas. Dentro de esta se encuentra información de clientes, empleados o información que se tiene obligación legal de proteger. También cae en esta categoría cualquier información que la Dirección estime que proporciona una ventaja competitiva o la

que sí es divulgada a entidades no autorizadas pudiera ocasionar un perjuicio a Grupo SUSESS y/o a sus clientes.

INFORMACIÓN PÚBLICA: es la que es libremente disponible tanto al interior como al exterior y que fue creada con el propósito de su uso público, como, por ejemplo: folletos, anuncios o la página web.

INFORMACIÓN RESTRINGIDA: información que si es divulgada a entidades no autorizadas podría tener un impacto en obligaciones legales o regulatorias para la empresa o para sus clientes.

RECURSOS IT: Un término que describe de manera amplia toda la infraestructura de Tecnologías de la Información, software y/o hardware con capacidades de cómputo y trabajo en red. Está incluido, pero no limitado a: sistemas y dispositivos de computación portátil, teléfonos móviles, impresoras, dispositivos de red, sistemas de control industrial, sistemas de control de acceso.

CONFIDENCIALIDAD: Proteger información institucional de la divulgación no autorizada.

INTEGRIDAD: Mantener la exactitud y confiabilidad de la información.

DISPONIBILIDAD: Asegurar que la información y los servicios que la proporcionan estén disponibles para los usuarios.

6. POLÍTICA

Grupo SUSESS contempla que la información, en cualquiera de sus formas, constituye un activo de la empresa y por lo tanto requiere de controles adecuados para protegerla de todas las amenazas internas o externas.

La información es de vital importancia para un funcionamiento eficiente y efectivo de la organización en el contexto actual de un mundo colaborativo que depende de compartir información electrónica. Dicha información solo debe utilizarse para los fines establecidos, es decir, para las operaciones comerciales de Grupo SUSESS, en particular el proceso de desarrollo de software en todas sus etapas: producción, venta, implementación y soporte.

El objetivo de la política de seguridad en la información de Grupo SUSESS es proporcionar acceso a la información únicamente a quienes tengan una base probada de uso de la información empresarial creada, recibida o recolectada (Información Institucional) y denegar el acceso a todos los demás, con el propósito de mantener su integridad, esto aplica tanto a socios, directivos, personal, clientes y proveedores.

Es también objetivo de la política de seguridad en la información de Grupo SUSESS garantizar la continuidad del negocio y minimizar el impacto de los incidentes de seguridad de la información, asegurando que mantenemos los siguientes aspectos de la misma:

CONFIDENCIALIDAD.

INTEGRIDAD.

DISPONIBILIDAD.

La alta dirección de Grupo SUSESS destinará los recursos necesarios para cumplir con los requisitos mínimos de configuración segura para todos los sistemas y aspectos mencionados previamente entre los que se incluyen equipamiento, capacitación de personal, pruebas y auditorías del SGSI.

Así mismo, la alta dirección realizará anualmente la planificación para de los objetivos de esta política, asignando los recursos, responsabilidades, plazos y mediciones correspondientes para asegurar su consecución.

Es compromiso de Grupo SUSESS para lograr el adecuado cumplimiento de esta política y de sus objetivos conservar toda la información documentada, los registros de seguimiento y los registros de las acciones de corrección y mejora emprendidos.

Esta política debe comunicarse de manera apropiada a todas las partes involucradas.

7. ROLES Y RESPONSABILIDADES

Esta sección establece el conjunto de responsables de la implementación del Sistema de Gestión de Seguridad de la Información, así como las responsabilidades correspondientes a cada uno.

PUESTO	**RESPONSABILIDADES**
DIRECTOR GENERAL	Responsable de la seguridad del sitio, incluyendo la seguridad física, de la información y la continuidad del negocio. Responsable de las revisiones de seguridad de la información para las auditorías.
GERENTE DE SISTEMAS Y CIBER SEGURIDAD	Líder del programa de seguridad del SGSI es el aprobador del SGSI. Responsable de la aprobación de los documentos, registros y dirección del SGSI.
JEDE DE AUDITORIA INTERNA	Responsable de las verificaciones internas del cumplimiento del SGSI.

INGENIERIO DE CIBER SEGURIDAD	Responsable de la implementación y ejecución del SGSI. Debe identificar y mitigar las amenazas que se presenten en la operación del negocio.
OFICIAL DE PROTECCIÓN DE DATOS	Es responsable de que las leyes aplicables a la privacidad de datos se cumplan para la información de terceros.

8. PRINCIPIOS GENERALES

8.1. LINEAMIENTOS PARA ASEGURAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Con el propósito de asegurar la confidencialidad de la información se establecen las siguientes políticas, procedimientos y controles como parte de esta política:

- Política de Clasificación de la Información
- Procedimiento de Etiquetado de la Información
- Procedimiento de Manejo de la Información
- Acuerdos de confidencialidad entre Grupo SUSESS y cada uno de los miembros del personal que tengan o que pudieran llegar a tener acceso a información confidencial, formando parte de esta de manera a priori cualquier pieza del desarrollo del software de control volumétrico regulado por el Anexo 30 de la Resolución Miscelánea Fiscal de 2019 y por el SAT
- Acuerdos de confidencialidad entre Grupo SUSESS y cada uno de los proveedores de servicios que tengan o que pudieran llegar a tener acceso a información confidencial de manera explícita o por el simple hecho de que llegara a estar almacenada en dispositivos alojados en sus instalaciones, formando parte de esta de manera a priori cualquier pieza del desarrollo del software de control volumétrico regulado por el Anexo 30 de la Resolución Miscelánea Fiscal de 2019 y por el SAT

Los activos de información o de TI que Grupo SUSESS adquiera o contrate, incluyendo servicios basados en la nube, deben cumplir con los siguientes requerimientos:

- ser basados en estándares
- ser efectivos y seguros
- soportar implementaciones modulares tales como:
  - ✓ implementaciones multiproveedor
  - ✓ capacidades de seguridad implementadas de manera independiente

8.2. ASPECTOS CONTRACTUALES CON PROVEEDORES Y CONTRATISTAS

Todas las relaciones comerciales con proveedores y contratistas que tengan relación con productos o servicios de TI deben apegarse a los lineamientos establecidos por esta política.

Además del acuerdo de confidencialidad establecido en el punto anterior, en los contratos correspondientes y cuando sea aplicable se incluirán clausulas en las que se establezca la obligatoriedad de parte del proveedor o contratista de permitir y participar en auditorías a sus procesos de suministro de productos o servicios.

8.3. PROPIEDAD INTELECTUAL

En todas las relaciones contractuales tanto con proveedores, contratistas, clientes y empleados se deberán establecer todos los derechos de propiedad intelectual que Grupo SUSESS tenga o pudiera llegar a tener en el momento y con motivo de la celebración del contrato.

En el caso de que se realice una transferencia de los derechos de propiedad intelectual de Grupo SUSESS esta deberá mencionarse explícitamente.

Cuando los contratos correspondientes no tengan relación con transferencias de derechos de propiedad intelectual de Grupo SUSESS este hecho deberá quedar expresado claramente.

En el caso de que los contratos tengan relación con otorgamiento de licencias de productos cuya propiedad intelectual pertenezca a Grupo SUSESS el alcance de la licencia deberá quedar claramente expresada en dichos contratos.

Los derechos de propiedad intelectual a que se refiere este apartado incluyen:

- Patentes
- Marcas
- Derechos de autor

9. MECANISMOS DE CONTROL

Por el hecho de que cualquier organización evoluciona y cambia debido tanto a influencias internas como externas, es necesario que el SGSI sea capaz de ajustarse a los cambios organizacionales para mantenerse relevante y útil. Esta condición puede alcanzarse adoptando el ciclo Planificar – Hacer – Verificar – Actuar (PHVA), el cual puede describirse como sigue:

PLANIFICAR: definir la política, objetivos, procesos, procedimientos y controles, así como identificar problemas y administrar los riesgos, todo con el fin de soportar la entrega segura de información alineada con el negocio.

HACER: implementar y operar los procesos planificados.

VERIFICAR: monitorear, medir, evaluar y revisar los resultados tomando como referencia los objetivos y la política de seguridad de la información, de tal forma que puedan definirse y autorizarse acciones correctivas y de mejora.

ACTUAR: realizar acciones para asegurarse que la entrega de información segura se está logran-do y mejorar dicha entrega.

9.1. MEDICIÓN

- Elaborar y mantener registro de las acciones y eventos que tengan la posibilidad de impactar al SGSI.
- Monitorear y registrar intentos de ataques a la seguridad tanto fallidos como exitosos.
- Aplicar y registrar las acciones correctivas y de mitigación cuando se detecte una vulnerabilidad.
- Revisar la eficiencia de las acciones emprendidas del SGSI.
- Presentar a la alta dirección indicadores de desempeño del SGSI para determinar la adecuación y la mejora continua de los controles.

9.2. AJUSTE

La alta dirección en base a los indicadores de desempeño del SGSI emprenderá las acciones correspondientes para lograr su mejora continua

9.3. MEDIDAS DISCIPLINARIAS

- Llamada de atención verbal

- Extrañamiento por escrito con copia al expediente del involucrado
- Sanción económica.

10. ANEXOS

Normatividad y Legislación:

- Anexo 30 de la Resolución Miscelánea Fiscal del 2019
- ISO 27001:2013
- Código Fiscal de la Federación
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Anexos

Forman parte del Sistema de Gestión de Seguridad de la Información los siguientes documentos:

- Política de Clasificación de la Información.
- Política de Uso Aceptable.
- Política de Control de Acceso.
- Procedimiento de Manejo de Incidentes de Seguridad.
- Política de Clasificación de Información.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Revisiones y Ajustes:

Este documento será válido durante 6 meses, para volver a ser válido deberá pasar por una revisión, la cual marcará los cambios realizados en contraste con su versión antigua. Estas revisiones serán echas periódicamente 6 meses después del último cambio realizado. Además, se podrá solicitar un cambio excepcional a causa de cambios importantes en la empresa, suceso inesperados o preparación ante regulaciones próximas.