POLÍTICA SEGURIDAD

GESTIÓN DE LA INFORMACIÓN

VERSION 7

Compusof s.a.

1 INDICE

2 ALCANCE

La presente política de seguridad de la información (en adelante política), se dicta en cumplimiento de las disposiciones legales vigentes, con el objetivo de gestionar adecuadamente la seguridad de la información, los sistemas informáticos, los procedimientos y el ambiente tecnológico de Compusof, S.A. (en adelante Compusof).

Debe de ser divulgada, conocida y cumplida por toda la plantilla del personal de Compusof, sea cual fuere su nivel jerárquico y a la totalidad de los procesos, ya sean internos o externos vinculados a Compusof a través de contratos o acuerdos con terceros.

La dirección es responsable de impulsar la implementación de la presente política, así como de la aprobación y cumplimiento de dicha política por parte de los empleados. Así como de la autorización de sus modificaciones.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política vigente.

El incumplimiento de la política de seguridad tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características del aspecto no cumplido, siendo dirección quien decida las sanciones en función de su gravedad.

3 TERMINOS Y CONDICIONES

A los efectos de este documento se aplican las siguientes definiciones:

3.1 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- **Confidencialidad de la información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente política, se realizan las siguientes definiciones:

- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas o audiovisuales.
- **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.
- **Tecnología de la información:** Se refiere al hardware y software operados por Compusof o por un tercero que procese información en su nombre, para llevar a cabo una función propia de Compusof, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otros.

3.2 Evaluación de Riesgos

Se realiza un análisis de riesgos de los activos y su plan de tratamiento de riesgos asociado.

3.3 Comité de Seguridad de la Información

El comité de seguridad de la información, está integrado por representantes de las áreas de IT, Dpto. Técnico y dirección de Compusof, destinado a garantizar el apoyo manifiesto de la dirección a las iniciativas de seguridad.

3.4 Responsable de Seguridad Informática

Es la persona que cumple la función de supervisar el cumplimiento de la presente política y de asesorar en materia de seguridad de la información a los integrantes de Compusof que así lo requieran.

3.5 Incidente de Seguridad

Es un evento adverso en un sistema de ordenadores o de red, que comprometa la confidencialidad, integridad o disponibilidad de la información. Puede ser causado mediante la explotación de alguna amenaza de romper los mecanismos de seguridad existentes.

3.6 Revisión de la Política de Seguridad

Compusof considera la revisión de la política de Seguridad y políticas asociadas a la preservación de la información dentro de la organización (y descritas dentro de la Política de Seguridad).

Anualmente, se realizará una revisión de esta Política de Seguridad además de llevarse a cabo siempre que se produzca algún cambio significativo en el sistema, con objeto de que dicha Política se mantenga actualizada y adecuada a la organización.

4 GENERALIDADES Y OBJETIVOS

4.1 GENERALIDADES

Partiendo de la base de que la información es un recurso que, como el resto de los activos, tiene valor para Compusof y por consiguiente debe ser debidamente protegida.

Es importante recordar que los principios de la política de seguridad son parte de la cultura de Compusof.

Para esto, existe un compromiso manifiesto de la dirección de Compusof, y de los directores de cada una de las distintas unidades de negocio, para la difusión y cumplimiento de la presente política.

4.2 OBJETIVOS

Respecto a seguridad de la información, las líneas estratégicas que Compusof ha definido y en la que se basan los objetivos del Sistema de Gestión, son los siguientes:

- Proteger los recursos de información de Compusof y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad de la información.
- Asegurar la implementación de las medidas de seguridad comprendidas en esta política, identificando los recursos correspondientes.
- Mantener la política de seguridad de Compusof actualizada, a efectos de asegurar su vigencia y nivel de eficiencia.

5 COMITÉ Y RESPONSABLES

5.1 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

La dirección de Compusof, configurara el comité de seguridad con los siguientes integrantes.

Área / Dirección	Representante
Dirección	Moisés Camarero Aguilar
Dpto. Técnico	Eduardo Fernandez
Responsable de TI	Pedro González
RRHH	Daniel Anton

5.2 ASIGNACIÓN DE RESPONSABILIDADES

Los responsables del cumplimiento de cada uno de los aspectos de esta política que son de aplicación a los procesos de seguridad y/o activos, son en cada caso:

Proceso	Responsable
Seguridad física y ambiental	Dirección
Seguridad del personal	RRHH
Control de accesos	RRHH
Seguridad en el mantenimiento de sistemas	Responsable de TI
Seguridad en las comunicaciones y las operaciones	Responsable de TI
Planificación de la continuidad operativa	Dpto. Técnico

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada y proporcionada al responsable de seguridad.

6 POLITICAS

6.1 CONFIDENCIALIDAD

- No comunicar a terceros datos relevantes de la compañía
- Ser responsable con la información/sistemas que se manejan
- Hacer uso del sentido común

6.2 INVENTARIO DE ACTIVOS

Se han identificado los activos de cada servicio y sus propietarios, elaborando un inventario con dicha información y será revisado con una periodicidad de 1 año.

6.3 SEGURIDAD EN LOS PUESTOS DE TRABAJO

Compusof ha determinado los niveles de acceso, derechos y restricciones de cada usuario en función de la actividad que cada uno realiza. Igualmente, el Responsable de Seguridad lleva a cabo análisis periódicos de verificación de los permisos de acceso y usuarios.

Respecto a puestos de trabajo, se debe de considerar siempre cumplir con las directrices de:

- No divulgar las contraseñas
- Proteger siempre el puesto de trabajo (bloqueo de sesiones).
- No utilizar los equipos para un uso que no sea el especifico del trabajo

6.4 DISPOSITIVOS MÓVILES

Se ha transmitido por medio del manual de seguridad a toda la organización, la sistemática de trabajo fuera de las oficinas de Compusof para preservar y asegurar que no se vea comprometida la información de negocio por trabajar con dispositivos móviles en entornos desprotegidos.

6.5 TELETRABAJO

Compusof ha implementado y establecido en el manual de seguridad, las medidas de seguridad necesarias para la protección de la información a la que se accede, tratan o almacena fuera de las oficinas, por medio de conexión VPN para los trabajadores con autorización.

6.6 COMUNICACIÓN DE INCIDENTES Y DEBILIDADES RELATIVOS A LA SEGURIDAD

Los incidentes y debilidades relativas a la seguridad serán comunicados a través de aplicación de gestión de servicios, teléfono y correo electrónico tan pronto como sea posible al responsable de seguridad.

6.7 PERÍMETROS DE SEGURIDAD FÍSICA

- Verificar la existencia de un área de recepción atendida por personal. Los métodos implementados registrarán cada ingreso y regreso en forma precisa.
- Identificar claramente todas las puertas de incendio de un perímetro de
- Las áreas protegidas se resguardan mediante el empleo de controles de acceso físico a fin de permitir el acceso sólo al personal autorizado.

6.8 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Se desarrollan procedimientos adecuados de controles de acceso al sistema y se consideran las siguientes acciones:

a) Instalar y actualizar periódicamente software de detección y reparación de virus, examinando los ordenadores y medios informáticos, como medida de prevención y rutinaria.

b) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles.

c) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

6.9 RESGUARDO DE LA INFORMACIÓN

El responsable del área informática dispondrá y controlará la realización de copias de respaldo de toda la información y del software crítico de Compusof.

Los sistemas de resguardo son comprobados periódicamente.

Cada usuario es responsable de los datos almacenados en su equipo de trabajo.

6.10 ADMINISTRACIÓN DE LA RED

Existen controles para garantizar la seguridad de los datos y los servicios conectados en las redes de Compusof, contra el acceso no autorizado.

Se restringe el acceso a los datos y aplicaciones solo al personal debidamente autorizado.

6.11 SEGURIDAD DE LOS MEDIOS EN TRANSITO

Los procedimientos de transporte de medios informáticos entre diferentes puntos (mensajería) deberán contemplar:

a) La utilización de servicios de mensajería confiables.

b) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible:

    1. Uso de recipientes cerrados.

    2. Entrega en mano.

6.12 SEGURIDAD EN EL CORREO ELECTRÓNICO

El correo electrónico es una herramienta más de trabajo provista al empleado con el fin de ser utilizada conforme al uso al cual está destinada, faculta a Compusof a implementar sistemas de controles destinados a velar por la protección y el buen uso del servicio.

Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, Compusof debe informar claramente a sus empleados:

a) Cuál es el uso que Compusof espera que los empleados hagan del correo electrónico provisto por Compusof

b) Bajo qué condiciones los mensajes pueden ser objeto de control y monitorización.

Normas y procedimientos claros con respecto al uso del correo electrónico, que incluyen los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo, virus, intercepción, etc.

b) Protección de archivos adjuntos de correo electrónico.

c) Aspectos operativos para garantizar el correcto funcionamiento del servicio

d) Potestad de Compusof para auditar los mensajes recibidos o emitidos por las cuentas de correo de Compusof.

6.13 INTERCAMBIO DE INFORMACIÓN

Cuando se realicen acuerdos entre organizaciones para el intercambio de información, se especificarán el grado de sensibilidad de la información de Compusof involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

a) Información sobre la propiedad de la información suministrada y las condiciones de su uso.

b) Normas técnicas para la grabación y lectura de la información

c) Controles especiales que puedan requerirse para proteger ítems sensibles.

Serán tenidas en cuenta todas las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en el "Documento de Seguridad COMPUSOF", así como las obligaciones del personal y los procedimientos de notificación, gestión y respuesta ante las incidencias.