

1. INTRODUCCIÓN

La Alta Dirección de Focus On Services está comprometida con el cumplimiento de los niveles, calidad de los servicios, y la protección de la información de las partes interesadas, asegurando su confidencialidad, integridad y disponibilidad, por lo cual se proporciona los recursos necesarios para establecer, mantener y mejorar continuamente su sistema de gestión, proporcionando mecanismos eficaces para asegurar que la entrega de los servicios y la protección de la información se encuentren alineados a la dirección estratégica y cumplan con los requisitos legales, contractuales, reglamentarios, y normativos aplicables.

2. ALCANCE

Focus On Services S.A de C.V tiene como misión proporcionar servicios y productos integrados asociados a las Tecnologías de la Información que satisfagan los requisitos y expectativas de clientes internos y externos en sectores públicos y privados, por lo tanto, esta política es aplicable a empleados, clientes internos y externos, proveedores o personas que actúen en nombre de la organización y del Sistema Integral de Gestión de Focus On Services (SIG-FOS).

3. OBJETIVOS

1. Incrementar en un 20% el conocimiento de los colaboradores sobre la importancia de la seguridad de la información dentro de la organización.
2. Garantizar la continuidad de las operaciones de la organización en caso de incidentes de seguridad de la información.
3. Asegurar la atención, seguimiento y cierre oportuno de todos los incidentes de seguridad de la información reportados a la Mesa de Servicio en un plazo máximo de 5 días hábiles.
4. Asegurar que el SIG-FOS cumpla con los requisitos de la norma ISO/IEC 27001 y los Controles del Anexo A aplicables a la organización.
5. Disminuir en un 15% el nivel de riesgo de los activos de información de la organización.

4. DEFINICIONES

- **Activo:** Cualquier cosa que tenga valor para la organización
- **Anexo A:** Lista de controles de seguridad de la información, que sirven como guía para que las organizaciones seleccionen e implementen medidas para gestionar riesgos de seguridad.
- **Confidencialidad:** Propiedad que determina que la información no está disponible ni sea revelada a quien no esté autorizado.
- **Control:** Medida que mantiene y/o modifica un riesgo.
- Disponibilidad Propiedad que la información sea accesible y utilizable por solicitud de los autorizados
- **Incidente de seguridad de la información:** evento o serie de eventos relacionados e identificados como eventos de seguridad de la información que pueden dañar a los activos de la organización o comprometer sus operaciones.
- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos.
- **ISO/IEC 27001:** Norma internacional líder para Sistemas de Gestión de Seguridad de la Información.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Usuario:** Persona o entidad que tiene acceso a los sistemas de información y a los datos de una organización.

5. RESPONSABILIDADES

- La Alta dirección es responsable de:
 - Establecer y mantener un marco de seguridad de información y alinear esta política de acuerdo a las necesidades de la organización.
 - Revisar anualmente la política para garantizar su efectividad y relevancia.
 - Definir los roles y responsabilidades del Comité de Seguridad de la Información.
- El Oficial de Seguridad de la Información:
 - Supervisar el cumplimiento de esta política, comprometiéndose a promover, comunicar y generar conciencia sobre la Seguridad de la Información.
 - Asignar responsables para coordinar la respuesta a incidentes y mitigar cualquier impacto negativo en la organización.
- Todos los colaboradores, clientes y proveedores deben cumplir con esta política y proteger la información confidencial a la que tengan acceso.

6. DESCRIPCIÓN DE LA POLÍTICA

1. La organización se compromete a revisar el cumplimiento y desempeño de su Sistema Integral de Gestión con la finalidad de adecuarlo y mejorarlo continuamente.
2. Se realizan auditorías internas y externas para verificar el cumplimiento de políticas, controles de seguridad implementados y de los requisitos aplicables de la norma ISO/IEC 27001.
3. La organización define controles de seguridad de tipo organizacional, personal, físico y tecnológico para proteger la información contra accesos no autorizados, pérdida o daño.
4. Se definen y asignan permisos de acceso para poder ingresar a las instalaciones, zonas, redes, hardware o software de acuerdo a su puesto, rol o perfil de la persona que desee ingresar o hacer uso de los activos de la organización.
5. Los colaboradores, clientes, proveedores y visitantes que ingresen a las instalaciones de la organización deben portar en un lugar visible sus respectivas credenciales para su correcta identificación.
6. Una vez que se finalice el servicio (conclusión de un servicio, término de relación laboral o comercial) en los equipos de cómputo, se eliminará en un período que no exceda los 90 días toda información personal del usuario.
7. Se mantendrán registros de acceso para supervisar la actividad de los usuarios y detectar posibles infracciones de seguridad.
8. Los equipos (computadoras, laptops, dispositivos móviles) son para uso exclusivo de las funciones laborales, para las que fue contratado el colaborador.
9. Cualquier incidente de seguridad, como el robo de un equipo, la pérdida de información o la sospecha de un ataque informático, debe ser reportado de inmediato al Oficial de Seguridad de la Información.
10. Los empleados son responsables de proteger la información de acuerdo con su clasificación. La información confidencial no debe ser almacenada en dispositivos personales ni compartida fuera de la red de la empresa sin la debida autorización.
11. Se mantendrá actualizado el procedimiento de Gestión de Seguridad de la Información para informar y responder a incidentes de seguridad de la información de manera oportuna y eficaz.

12. El procedimiento de Gestión Cambios se debe asegurar que en las solicitudes de cambio identifique los impactos potenciales en la seguridad de la información y la evaluación de los riesgos asociados.
13. Se comunicará a toda la organización la presente política y aquellas políticas derivadas de los controles de seguridad identificados en el Anexo A de la norma ISO/IEC 27001.
14. La política de seguridad de la información será comunicada a los colaboradores de Focus On Services mediante comunicados vía correo electrónico y ser proyectada en las pantallas de las instalaciones de la organización.
15. La presente política se comunicará de acuerdo a las necesidades del negocio por correo electrónico a clientes, proveedores y socios de negocios, y estará disponible para su consulta en la página oficial de Focus On Services.

7. INCUMPLIMIENTO Y SANCIONES

En caso de infringir la Política de Seguridad de la Información, se aplicará la Matriz de Sanciones, de acuerdo al procedimiento de Administración de Personal y Gestión de Seguridad de la Información para evaluar y determinar las consecuencias administrativas, laborales o legales aplicables.

Atentamente

Carlos A. Lucio Navarro

 Oficial de Seguridad de la Información

Francisco J. Lucio Sandoval

 Director General

8. REVISIONES Y APROBACIONES

ELABORÓ	REVISÓ	AUTORIZÓ
Carlos A. Lucio Navarro	Verónica Islas García	Francisco J. Lucio Sandoval
Gerente de Preventa de Consultoría de Infraestructura de TI	Coordinador de Calidad y Servicios	Director General

9. CONTROL DE CAMBIOS DE LA POLÍTICA

FECHA DEL CAMBIO	VERSIÓN	SECCIÓN MODIFICADA	TEXTO MODIFICADO
22-Oct-20	00	Todo	Se presenta documento por primera vez para su uso, integrando las normas ISO 9001:2015 e ISO/IEC 20000-1:2018.
27-Abr-22	01	Objetivos de seguridad de la información del SIG-FOS	Se agrega Inciso 5 de acuerdo a la política de retención de datos.
15-Sep-25	02	Todo	Reestructuración de la política.