INFOCENTER

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

1. GENERAL

La información que genera y gestiona INFOCENTER S.A., constituye un activo estratégico clave para asegurar la continuidad del negocio. En este contexto, la Política de Seguridad de la Información está orientada a proteger la información, los medios que permiten dicho ciclo y las personas que acceden a la información y/o la manipulan, con el fin de garantizar su integridad, disponibilidad y confidencialidad.

1.1. OBJETIVO

Desarrollar, implementar y gestionar un sistema de gestión de seguridad de la información, alineado a la misión y objetivos de la organización, protegiendo los activos de la información, el uso adecuado de los recursos, la gestión de los riesgos y la continuidad del negocio.

1.2. ALCANCE

Toda persona cuya actividad pueda, directa o indirectamente, interna o externamente, verse afectada por los requisitos del Sistema de Gestión de la Seguridad de la Información, está obligada al cumplimiento estricto de la Política de Seguridad de la Información.

2. CONTENIDO

En INFOCENTER S.A. la información es un activo esencial para la prestación de sus servicios por ello reconoce la importancia de implementar controles y destinar recursos para resguardar los activos de información más significativos.

En consecuencia, se compromete establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información según la Declaración de Aplicabilidad (GIR-FM11-2018) como proceso.

Los trabajadores, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre activos de información de INFOCENTER S.A., deberán adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

Estos conceptos fundamentales constituyen la base de la seguridad de la información:

Confidencialidad: Garantiza que sólo aquellos que están autorizados a acceder a la información pueden hacerlo.

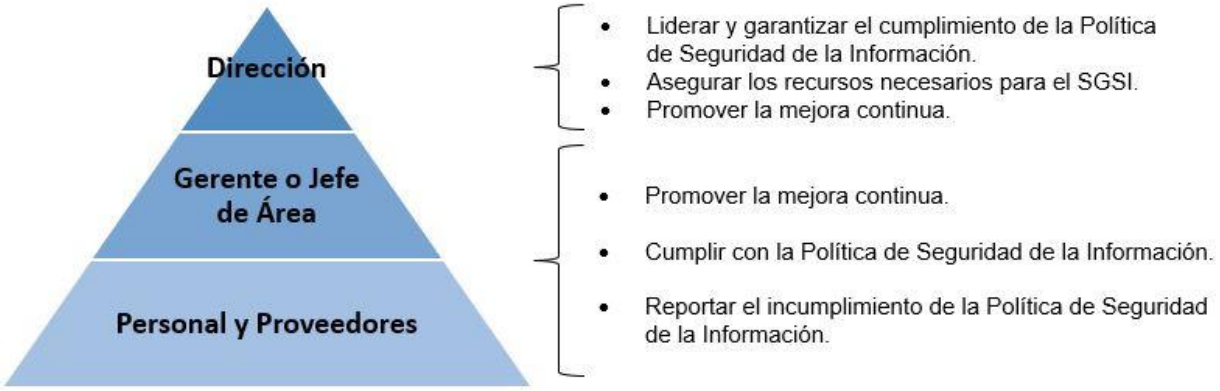
Integridad: Garantiza que los usuarios o procesos no autorizados no realizan modificaciones en los datos conservando la exactitud e integridad de la información y los métodos de procesamiento.

Disponibilidad: Garantiza que los usuarios tengan acceso oportuno a la información, sistemas y activos asociados, cuando sea necesario.

La Política de Seguridad de la Información se encuentra soportada por reglamentos, políticas y procedimientos específicos los cuales guiaran el manejo adecuado de la información de INFOCENTER S.A.

Organización de la Seguridad de la Información

La alta dirección, como todo el personal y proveedores, cumplen con un rol importante en la gestión de seguridad de la información.



Se designará al Oficial de Seguridad de la Información "OSI", como Responsable de la Seguridad de la Información, gestionando con las instancias que correspondan la implementación, revisión del cumplimiento, actualización y difusión de las Políticas y los Procedimientos de Seguridad de la Información. Asimismo, mantener contacto con autoridades y grupos especiales de interés para su mejora continua.

2.1. ADMINISTRACIÓN DE SERVICIOS Y CONTRATOS CON TERCEROS

La contratación de servicios externos que requieran acceso a la información clasificada como privada y/o confidencial deberá considerar medidas que aseguren la calidad y minimicen el nivel de riesgo de dicho servicio.

Se define lo siguiente:

- Evaluar y seleccionar los proveedores bajo procesos formalmente establecidos.
- Asegurar que el proveedor cuente con la experiencia y capacidad necesaria para responder a las características del servicio que se desea contratar.
- Para casos de procesamiento de datos o ejecución de sistemas en lugar externo verificar que el proveedor cuente con los sistemas e infraestructura tecnológica suficiente para ofrecer continuidad operacional, confidencialidad, integridad, exactitud y calidad de la información y datos.
- Especificar en los contratos la responsabilidad que asume la empresa proveedora de procesamiento externo en caso de ser vulnerados sus sistemas, ya sea por ataques internos, externos, deficiencias o fallas.
- Exigir a los proveedores el cumplimiento de las políticas y procedimientos de seguridad de la información pertinentes.
- Asegurar las medidas necesarias de continuidad operacional, en caso de cambio de proveedor externo u otro factor no previsto.
- Practicar evaluaciones periódicas en las empresas proveedoras de los servicios, directamente o mediante auditorías independientes.
- Reconsiderar los riesgos y controles asociados antes de adquirir un producto que no satisface los requisitos de seguridad de la información que se indican en el contrato.
- Exigir al proveedor los acuerdos de confidencialidad firmados con su personal que participa en el proyecto de desarrollo de programas, sistemas o aplicaciones.
- Asegurar que la empresa contratada para el desarrollo y mantenimiento de programas y aplicaciones cuente con solidez financiera, organización, licencias de sistemas operativos y herramientas que se utilizarán en el desarrollo, además de personal con conocimiento y experiencia.

- Aclarar con el proveedor, a quién pertenece la propiedad intelectual en caso de desarrollo de programas, sistemas o aplicaciones.
- Establecer Acuerdos de Nivel de Servicio en los contratos, de acuerdo al análisis de riesgo tecnológico y de acuerdo a la criticidad de sus operaciones.
- Los trabajadores de otras empresas y/o instituciones deberán adecuarse al horario laboral de INFOCENTER S.A., excepto bajo solicitud expresa para trabajar en horarios fuera de oficina.
- Los trabajadores de otras empresas y/o instituciones que requieran conectar sus equipos de trabajo a la red interna deberán mostrar las licencias del software que corresponda.

2.2. CUMPLIMIENTO REGULATORIO DE SEGURIDAD DE LA INFORMACIÓN

INFOCENTER S.A. estará alienado a las disposiciones legales y normativas o aquellas contractuales relacionadas a sistemas de información y tecnologías que las soportan, a fin de evitar sanciones o conflictos para la empresa.

Se define lo siguiente de acuerdo a requisitos legales, regulatorios y contractuales:

- Identificar los requisitos que sean importantes para los sistemas de información.
- Garantizar el cumplimento para el uso de material con derechos de propiedad intelectual asociados y para el uso de software propietario.
- Garantizar la protección y privacidad de los datos.
- Proteger los registros y pistas de auditoría de la pérdida, destrucción y falsificación.
- Disuadir a los usuarios sobre el uso de los recursos de información para propósitos no autorizados.
- Los Gerentes y/o Jefes de áreas deberán asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente y cumplen con las políticas de seguridad.
- Efectuar auditorías internas y/o externas sobre el cumplimiento de las políticas de seguridad de la información.

3. COMUNICACIÓN

Infocenter reconoce la importancia de comunicar de forma efectiva la información y los asuntos relacionados con la seguridad de la información a todas las partes interesadas internas y externas de forma oportuna y precisa. Siendo el Oficial de Seguridad de la Información el encargado de la comunicación ya sea por correo electrónico u otro medio a los trabajadores según corresponda la necesidad y su frecuencia. El uso y medios de comunicación para la difusión, concientización y evaluación sobre seguridad de la información se realizarán según el plan de concientización del Oficial de Seguridad de la Información.

4. SANCIONES POR INCUMPLIMIENTO

El cumplimiento de la Política de Seguridad de la Información y/o procedimientos que se desprenden de la misma es obligatorio para Directivos, Ejecutivos y Trabajadores según corresponda, la no observación de lo establecido en ella estará sujeta a sanciones definidas en el Código de Ética, Gobierno Corporativo y Reglamento Interno de Trabajo según corresponda.

Las sanciones para consultores y personal eventual serán definidas en los contratos de servicios.