



SISTEMA DE GESTIÓN INTEGRADO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN	FECHA	REGISTRO DE REVISIONES DEL DOCUMENTO
1	21/07/2023	Definición política de seguridad de la información
2	18/08/2023	Revisada por el Comité de Seguridad de la Información
3	22/08/2023	Aprobado por Gerencia General

ELABORADO POR	APROBADO POR
Oficial de Seguridad	Gerente General

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		VERSIÓN	1
			FECHA	21/07/2023
Referencia	ISO 27001:2022 ISO 9001:2015 ISO 14001:2015 ISO 45001:2018		PÁGINA	2 DE 5

INTRODUCCIÓN

Esta política establece las reglas y lineamientos esenciales para la administración, uso y protección de la información y los recursos informáticos asociados a su tratamiento. Se basa en normas y regulaciones nacionales e internacionales, así como en los lineamientos estratégicos de Dimacofi.

La dirección y el personal de Dimacofi entienden que la información propia, de los clientes y otras partes involucradas con la empresa es un recurso fundamental para la organización y, por consiguiente, asumen la responsabilidad que les corresponde por la adecuada protección de esta.

La seguridad de la información es la protección de esta de un amplio espectro de amenazas, sean estas humanas, naturales o cibernéticas. Su propósito es minimizar los riesgos del negocio, garantizar la continuidad operacional y maximizar el retorno sobre las inversiones y oportunidades de negocio de Dimacofi.

ALCANCE

Esta política es aplicable a todo el personal interno o externo que realice actividades para Dimacofi. Esto incluye:

- Los activos de información propiedad de Dimacofi o de sus clientes que se encuentren bajo la custodia o administración de Dimacofi.
- La infraestructura tecnológica que permite la generación, procesamiento, transmisión y almacenamiento de información.
- Las instalaciones físicas donde residen los activos de información.
- El personal que hace uso de los activos de información, sean estos colaboradores de Dimacofi, directores, personal ejecutivo, clientes, proveedores y contratistas.

OBJETIVOS

- Establecer requisitos que permitan la implementación de controles para la protección adecuada, razonable y efectiva de los activos de información durante el uso cotidiano de los mismos.
- Mantener la confidencialidad, integridad y disponibilidad de los activos de información de la compañía.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		VERSIÓN	1
			FECHA	21/07/2023
	Referencia	ISO 27001:2022 ISO 9001:2015 ISO 14001:2015 ISO 45001:2018		PÁGINA

- Identificar los riesgos que pudieran materializarse sobre los activos de información a través de una adecuada evaluación de estos, de forma de entender las vulnerabilidades y las amenazas a las cuales están expuestos.
- Gestionar los riesgos en un nivel aceptable a través del diseño, implementación y mejora continua de un Sistema de Gestión de la Seguridad de la Información.
- Favorecer la comunicación, sensibilización e información de los lineamientos de seguridad a todos los integrantes de la empresa.

DEFINICIONES

Activo de Información: Toda información o recurso relacionado para la creación, almacenamiento, manejo o transmisión de esta.

Confidencialidad: característica de la información por la cual solo está disponible para personas o sistemas autorizados.

Integridad: característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.

Disponibilidad: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

Incidente de Seguridad: Evento, o serie de eventos, indeseado e inesperado que tiene una alta probabilidad de poner en riesgo las actividades comerciales y de amenazar la seguridad de la información.

Dueño de activos de información: Persona o entidad con responsabilidad y autoridad para gestionar un activo de información.

Oficial de Seguridad de la Información: Responsable de desarrollar e implementar políticas y procedimientos para garantizar la seguridad e integridad de los sistemas de información de una organización. Identifica y mitiga riesgos, responde a incidentes de seguridad, asegura el cumplimiento de las leyes y regulaciones relevantes y trabaja en

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		VERSIÓN	1
			FECHA	21/07/2023
	Referencia	ISO 27001:2022 ISO 9001:2015 ISO 14001:2015 ISO 45001:2018	PÁGINA	4 DE 5

estrecha colaboración con otros ejecutivos e interesados para integrar la seguridad de la información en todos los aspectos de las operaciones de la organización.

REGLAS DE LA POLÍTICA

- Todo el personal de Dimacofi, sea permanente o temporal, tiene la obligación de proteger los activos de información, los sistemas y la infraestructura tecnológica de la organización, actuando siempre de forma responsable y profesional, manteniendo pleno conocimiento de lo establecido por la presente política.
- Todos los activos de información, al igual que los riesgos a los que están expuestos, deberán poseer un dueño designado, quien será responsable de asegurar que los mismos se encuentren debidamente inventariados y clasificados según su criticidad. Será también su responsabilidad realizar una revisión periódica de dicha clasificación y de las autorizaciones de acceso a los mismos.
- Todos los activos de información deberán ser protegidos en función de su clasificación y según lo definido por la evaluación de riesgos correspondiente.
- Todo proyecto que involucre activos de información deberá, desde su concepción, incorporar los requerimientos de seguridad definidos por el Oficial de Seguridad. El proceso de incorporación y validación de la seguridad deberá estar integrado a la administración de proyectos desde la etapa de diseño.
- Todo el personal de Dimacofi tiene la responsabilidad de notificar incidentes de seguridad y potenciales debilidades que pudieran detectarse.
- El Oficial de Seguridad será responsable de implementar un programa adecuado de sensibilización y capacitación. Este programa deberá estar disponible para todo el personal de Dimacofi, incluyendo empleados permanentes, temporales y externos.
- La dirección de la organización declara su decisión de mejorar continuamente los procesos y niveles de seguridad a través de un seguimiento permanente de los controles y procedimientos implantados. Del mismo modo, declara su intención de asegurar la existencia de planes de contingencia que permitan garantizar la continuidad de los servicios prestados por la compañía.
- La dirección de la organización declara su decisión de cumplir con la normativa y legislación vigente en temas de Seguridad de la Información y Ciberseguridad, y con los requerimientos contractuales establecidos por los clientes con relación a la misma.
- La dirección de Dimacofi será responsable de la gestión de los temas de Seguridad de la Información y Ciberseguridad, y tendrá la autoridad para su implantación, control y justificación de las desviaciones o excepciones que, por naturaleza del alcance, no apliquen.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		VERSIÓN	1
			FECHA	21/07/2023
	Referencia	ISO 27001:2022 ISO 9001:2015 ISO 14001:2015 ISO 45001:2018	PÁGINA	5 DE 5

- La dirección de Dimacofi declara su compromiso con la debida asignación de recursos para asegurar la adecuada gestión y mejora del SGSI.

REVISIÓN, VALIDACIÓN Y DIFUSIÓN

- Esta política deberá ser revisada anualmente por el Comité de Seguridad de la Información y actualizada cuando sea necesario. La misma deberá ser aprobada por el Gerente General.
- En caso de no existir modificaciones, ya sea a esta u otras políticas corporativas, deberá indicarse la justificación correspondiente en el registro de cambios del documento respectivo.
- Se difundirá esta política a todo el personal de Dimacofi actualmente contratado, a aquellos empleados que están siendo incorporados a la organización en forma permanente o transitoria, y a todas las partes interesadas del sistema de gestión.