

	<b>SISTEMA DE GESTIÓN DE PROCESOS</b>	Código: PO-TI-0002
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	Versión: 1
		Fecha de creación: 26/03/2020

## 1. Objetivo

La información debe ser siempre protegida, en cualquiera que sea su forma de ser compartida, digital, comunicada o almacenada.

La información puede existir en diversas formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en proyecciones o en forma oral en las conversaciones.

La seguridad de la información es la protección de la información contra una amplia gama de amenazas con el fin de garantizar la continuidad del negocio, minimizar los riesgos empresariales y maximizar el retorno de las inversiones y oportunidades de negocio.

## 2. Alcance

Esta política apoya la de Gestión de Seguridad de la Información de la organización.

Esta política es de consideración por parte de todos los miembros de la organización.

## 3. Lineamientos generales

1. Comprender y tratar los riesgos operacionales y estratégicos en seguridad de la información para que permanezcan en niveles aceptables para la organización.
2. La protección de la confidencialidad de la información relacionada con los clientes, empleados y con los planes de desarrollo de Mega Gasolineras, S.A. de C.V.
3. La conservación de la integridad de los registros de ventas, contables e información en general.
4. Los servicios Web de acceso público y las redes internas cumplen con las especificaciones de disponibilidad requeridas.
5. Entender y dar cobertura a las necesidades de todas las partes interesadas.
6. La seguridad Informática y protección contra ataques se encuentra protegida con un equipo de la marca WatchGuard modelo Firebox 360 cuyas políticas de seguridad se revisan constantemente, además de la actualización de riesgos y firmware de manera automática.
7. Todos los equipos cuentan con un antivirus instalado con licencia vigente y actualizado de manera automática de forma diaria.
8. Los puertos USB se encuentran bloqueados en corporativos para evitar extracción masiva de información.
9. El envío de información corporativa debe ser enviada únicamente por medio de los recursos proporcionados por la empresa (Correo, Software autorizado, Evitar uso de redes públicas)

	<b>SISTEMA DE GESTIÓN DE PROCESOS</b>	Código: PO-TI-0002
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	Versión: 1
		Fecha de creación: 26/03/2020

10. Todos los empleados deben tener firmado desde el momento de su contratación el aviso de privacidad, de uso de datos personales y organizacionales.

#### **4. Principios de seguridad de la información**

1. Esta organización afronta la toma de riesgos y tolera aquellos que, en base a la información disponible, son comprensibles, controlados y tratados cuando es necesario. Los detalles de la metodología adoptada para la evaluación del riesgo y su tratamiento se encuentran descritos esta política.
2. Todo el personal que tenga información confidencial y/o general será informado y responsable de la seguridad de la información, según sea relevante para el desempeño de su trabajo.
3. Se tendrán en cuenta aquellas posibilidades de fraude relacionadas con el uso abusivo de los sistemas de información dentro de la gestión global de los sistemas de información.
4. Se harán disponibles informes regulares con información de la situación de la seguridad.
5. Los riesgos en seguridad de la información serán objeto de seguimiento y se adoptarán medidas relevantes cuando existan cambios que impliquen un nivel de riesgo no aceptable. El departamento de TI será el responsable de la revisión y aplicación de nuevos métodos que corrijan cualquier fuga o información en riesgo.
6. Los criterios para la clasificación y la aceptación del riesgo serán clasificados como se detalla a continuación:
  - **Alto.** - Pone en riesgo la operación y/o la seguridad o integridad de las operaciones registradas o la integridad del personal.
  - **Medio.** - Puede existir fuga de información provocada por alguno de los colaboradores de la organización.
  - **Bajo.** - Se detecta una posibilidad de fuga de información y debe ser comunicada de forma inmediata con el jefe directo.
7. Las situaciones que puedan exponer a la organización a la violación de las leyes y normas legales no serán toleradas.
8. Queda a criterio de la Gerencia de TI en conjunto con Dirección y el área involucrada las acciones a tomar en cualquiera de las clasificaciones descritas previamente.

#### **5. Responsabilidades**

1. El equipo de TI es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la organización.
2. Cada gerente de área es responsable de garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la organización.

	<b>SISTEMA DE GESTIÓN DE PROCESOS</b>	Código: PO-TI-0002
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	Versión: 1
		Fecha de creación: 26/03/2020

3. La Gerencia de TI asesora al equipo directivo, proporciona apoyo especializado al personal de la organización y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.
4. **Cada miembro del personal tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.**
5. La Gerencia de TI será responsable de informar al Gerente de RH la infracción a cualquier de los puntos mencionados en esta política y/o cualquier situación que ponga en riesgo, dañe o provoque conflictos en la organización, relacionado con el uso indebido de la información.

**6. Indicadores clave:**

- Los incidentes en seguridad de la información se clasifican en ALTO, MEDIO o BAJO y las acciones a tomar deberán ser consensuadas y ejecutadas por el área correspondiente.
- Las pérdidas por fraude serán detectadas y permanecerán dentro de unos niveles aceptables.
- La aceptación del cliente de los productos o servicios debe ser afectada negativamente por aspectos relacionados con la seguridad de la información.

**Políticas relacionadas:** A continuación, se detallan aquellas políticas que proporcionan principios y guía en aspectos específicos de la seguridad de la información:

- Política de Manejo de videos (CCTV).

**Esta política debe ser comunicadas a los empleados y partes externas interesadas.**

**La Gerencia de Tecnologías de la Información de la empresa es la responsable de aprobar una política de seguridad de la información que asegure que:**

1. La información estará protegida contra cualquier acceso no autorizado.
2. La confidencialidad de la información, especialmente aquella relacionada con los datos de carácter personal de los empleados y clientes.
3. La integridad de la información se mantendrá en relación a la clasificación de la información (especialmente la de “uso interno”).
4. La disponibilidad de la información cumple con los tiempos relevantes para el desarrollo de los procesos críticos de negocio.
5. Se cumplen con los requisitos de las legislaciones y reglamentaciones vigentes, especialmente con la Ley de Protección de Datos y de Firma Electrónica.

	<b>SISTEMA DE GESTIÓN DE PROCESOS</b>	Código: PO-TI-0002
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	Versión: 1
		Fecha de creación: 26/03/2020

6. Los planes de continuidad de negocio serán mantenidos, probados y actualizados al menos con carácter anual.
7. La capacitación en materia de seguridad se cumple y se actualiza suficientemente para todos los empleados.
8. Todos los eventos que tengan relación con la seguridad de la información, reales como supuestos, se comunicarán al responsable y serán investigados.

**Las visitas y personal externo que accedan a nuestras instalaciones no están exentas del cumplimiento de las obligaciones** indicadas en la documentación la política, y el personal interno observará su cumplimiento.

En cualquier caso, de duda, aclaración o para más información sobre el uso de esta política y la aplicación de su contenido, consulte por teléfono 477 401 5457 o e-mail [jcarmona@megagas.mx](mailto:jcarmona@megagas.mx) al Gerente de Tecnologías de la Información quien ha sido designado formalmente en el organigrama corporativo.

DESCRIPCIÓN DE CAMBIOS			
FECHA DE CAMBIO	VERSIÓN A LA QUE CAMBIA	SOLICITANTE	BREVE DESCRIPCIÓN DEL CAMBIO
16/11/2021	1	Jesús Carmona	Actualización de Lineamientos generales
RESPONSABLES DE ELABORACIÓN, REVISIÓN Y APROBACIÓN			
ELABORÓ:	REVISÓ	AUTORIZÓ	
José de Jesús Carmona Ponce	Karina Godínez Serrano	Rodrigo Suárez R.	
Gerente de TI	GERENTE DE PROCESOS.	CEO	