GRUPO coremsa

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

GRUPO COREMSA corporación empresarial de ámbito nacional, en su afán de mejorar los servicios prestados y satisfacer las necesidades de sus clientes, ante la necesidad de mejorar la gestión ambiental y con el propósito de proteger los activos de información, ha implantado un sistema para la gestión integrada de la calidad, el medio ambiente y la seguridad de la información, de acuerdo con las normas ISO 9001, ISO 14001 e ISO 27001 en un número significativo de los centros de trabajo de las empresas que lo componen, con el objetivo de que le ayude a desarrollar una imagen de excelencia en las actividades y operaciones en las que interviene.

La Dirección General de GRUPO COREMSA asume el compromiso de liderar e impulsar la POLITICA DE GESTIÓN INTEGRADA y el sistema a través de:

Principios generales:

- Política de análisis, gestión y disminución del riesgo potencial grave. Se priorizarán las actuaciones sobre riesgos potenciales graves.
- Política de Tolerancia con las incidencias. Se investigará y sancionará aquellas actuaciones dolosas o imprudentes.
- Política de impacto reputacional mínimo. La incidencia reputacional en materia de seguridad debe tender a 0.
- Política de gestión de personas como activo de información que incluya medidas de sensibilización y/ o formación en materia de seguridad.
- Política de control y autorización de accesos. Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.
- Política de seguridad física de las instalaciones. Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- Política de criterios de seguridad de la información aplicados a la gestión de proveedores y en la adquisición de productos (sistemas y servicios)
- Protección de datos (inactivos y en tránsito/medios). Se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos.
- Prevención contra la conexión a través de sistemas interconectados
- Integridad y actualización de los sistemas. Mantener actualizados nuestros sistemas y asegurar la integridad de nuestra información.
- Seguridad integral. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.
- Control operacional. Controlar operacionalmente de forma eficaz las amenazas y riesgos sobre el activo y las instalaciones.
- Gestión por procesos. Organizar el sistema por medio de la implementación de los procesos de seguridad que se revisan y mejoran de forma continua
- Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.
- Cumplimiento Legal. Garantizar que nuestras operaciones y procesos actuales y

futuros cumplan con la legislación vigente en materia de seguridad de la Información

Principios particulares y responsabilidades específicas:

- Gestionar eficientemente las incidencias que afecten a la integridad, disponibilidad y confidencialidad de la información de la empresa.
- Implantar planes de continuidad del negocio que garanticen la continuidad de las actividades de la sociedad en caso de incidencias graves o contingencias.
- Gestionar los roles de los profesionales responsables del sistema de seguridad de la información para asegurar el nivel de profesionalidad necesario.
- Registro de actividad.
- Protección de los sistemas y de la comunicación: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

Fieles a estos principios, los preceptos a cumplir por las empresas certificadas del GRUPO COREMSA se recogen en nuestro Sistema de Gestión, que se declara de obligado cumplimiento.

Málaga, 5 junio del 2023

PRESIDENCIA DE GRUPO COREMSA