POLÍTICA DE SEGURIDAD

DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El presente documento tiene por objeto establecer la Política de Seguridad de la Información para el Grupo Gaselec, en base a los requisitos dispuestos en el estándar de seguridad de la información UNE – ISO/IEC 27001, asegurando así la confidencialidad, integridad y disponibilidad de sus sistemas de información y, por supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables.

Como punto fundamental de la política está la implantación, operación y mantenimiento de un SGSI basado en ISO 27001.

Los aspectos básicos de la política de seguridad son:

- Asegurar la confidencialidad, integridad y disponibilidad de la información.
- Cumplir todos los requisitos legales aplicables.
- Tener un plan de continuidad que permite recuperarse de un desastre en el menor tiempo posible.
- Formar y concienciar a todos los empleados en materia de seguridad de la información.
- Gestionar adecuadamente todas las incidencias ocurridas.
- Todos los empleados son informados de sus funciones y obligaciones de seguridad y son responsables de cumplirlas.
- Hay un responsable de seguridad encargado del sistema de gestión la seguridad de la información (SGSI) de la organización.
- Mejorar de forma continua el SGSI y por ende, la seguridad de la información de la organización.

OBJETIVOS

Marcar las pautas de alto nivel a seguir para que todos los tratamientos de información relativos a los procesos de negocio indicados en el alcance se realicen de forma segura y únicamente por personal autorizado, así como proteger la información de la organización ante posibles pérdidas de confidencialidad, integridad y/o disponibilidad.
Para todo ello, existe un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001, con unos objetivos definidos de forma clara y que deben ser revisados de forma anual.

ALCANCE

Los procesos de negocio definidos en el alcance del sistema de gestión de seguridad de la información (SGSI) y el personal implicado en los mismos.

PLANIFICACIÓN

En la fase de planificación se incluye como punto fundamental un estudio de la seguridad de la compañía a través de un análisis de riesgos y plan de tratamiento de riesgos.

IMPLANTACIÓN

En base a los resultados obtenidos en la fase de planificación se implantan unos controles de seguridad u otros, además de operar los procedimientos del SGSI para dar cumplimiento a las exigencias del estándar ISO 27001.

REVISIÓN

La política de seguridad de la información y el SGSI son revisados regularmente a intervalos planificados o si ocurren cambios significativos para asegurar la continua idoneidad, eficacia y efectividad de la misma. De forma genérica son revisados anualmente junto con los procesos de auditoría interna del SGSI.

MEJORA

Las posibles mejoras de la política de seguridad de la información y del SGSI son encontradas bien durante las fases de revisión o bien en base a aportaciones que se consideren interesantes tanto de personal del Grupo Gaselec, como de personal de la empresa consultora.
Todo el SGSI se enmarca dentro del ciclo de Deming (ciclo PDCA), basado en la planificación de actividades, su implantación y operación, su revisión y su posterior mejora. Todo ello aplicado a la seguridad de la información.

RESPONSABILIDADES ASOCIADAS A LOS ACTIVOS

Los propietarios o responsables de los activos son responsables de:

- Asegurar que la información y los activos que contengan o traten con información estén clasificados correctamente.
- Definir y comprobar de forma periódica que las restricciones de acceso y la clasificación de la información sea la correcta.

EQUIPOS INFORMÁTICOS Y DE COMUNICACIONES Y SUS PROGRAMAS DE SOFTWARE

Los usuarios de los sistemas informáticos del Grupo Gaselec deben esforzarse en hacer y promover un uso eficiente de los mismos a fin de evitar tráfico innecesario en la red e

interferencias con su trabajo o el de otros usuarios o con otras redes asociadas ni con los servicios que éstas ofrecen.

El uso de los sistemas del Grupo Gaselec quedará reservado para las actividades propias a desempeñar en su puesto de trabajo.

Se promoverá el uso responsable de la red interna del Grupo Gaselec.

Será responsabilidad de los propios usuarios la correcta custodia de los activos que tengan en posesión para el desempeño de sus labores contractuales.

PROTECCIÓN DEL CONOCIMIENTO

No podrán divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral con el Grupo Gaselec, tanto en soporte material como electrónico. Todos los compromisos anteriores deben mantenerse, incluso después de extinguida la relación laboral.

PROPIETARIOS DE LA INFORMACIÓN

El propietario de la información será cada una de las sociedades del Grupo Gaselec.

Sin embargo, será responsabilidad de los usuarios el correcto tratamiento, almacenamiento y no divulgación de la información a la que tengan acceso como consecuencia del desempeño de sus actividades laborales.

SEGURIDAD DE LA GESTIÓN DE RECURSOS HUMANOS

Se asegurará que todos los empleados, contratistas y los terceros entienden sus responsabilidades y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos puestos a su disposición.

Se asegurará que todos los empleados, contratistas y los terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano.

Se asegurará que todos los empleados, contratistas y los terceros abandonan la organización o cambian de puesto de trabajo de forma ordenada y sin comprometer la seguridad de la misma.

SEGURIDAD FÍSICA Y DEL ENTORNO

Se prevendrá todo tipo de acceso físico no autorizado, daños o intromisiones en las instalaciones y en la información del Grupo Gaselec

Se tomarán las medidas de seguridad necesarias para evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos o que puedan provocar la interrupción de las actividades de la organización.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

La política de seguridad relativa a la gestión de comunicaciones y operaciones se basa en las siguientes partes:

FILTRADO DE CONTENIDOS

El uso del sistema informático del Grupo Gaselec para acceder a redes privadas o públicas, se restringirá, eliminando el acceso a los temas que no estén directamente relacionados con la actividad y los cometidos del puesto de trabajo del usuario.

CORREO ELECTRÓNICO

Se hará un uso responsable del correo electrónico, así como de la información transmitida a través de este medio, preservando la integridad.
Cualquier fichero introducido en la red o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus o cualquier tipo de código malicioso.

CONTROL DE ACCESOS

Se controlará el acceso a los sistemas de información del Grupo Gaselec, para que solo sea realizado por personal autorizado y en las condiciones de seguridad que la organización ha decido operar.

IDENTIFICACIÓN Y AUTENTIFICACIÓN DE LOS USUARIOS

Se asegurará el acceso de un usuario autorizado y se prevendrá el acceso de usuarios no autorizados a los sistemas de información del Grupo Gaselec.

ACCESO A INTERNET

Se prevendrá el acceso no autorizado a los servicios de red para los usuarios que no hayan sido legitimados.
Se usarán métodos seguros de autenticación para conexiones externas por parte de usuario autorizados.
La información transmitida a través de redes de telecomunicaciones se hará de forma segura.

ADQUISICIÓN, DESARROLLO Y MATENIMIENTO DE SISTEMAS

La política de seguridad relativa a la adquisición, desarrollo y mantenimiento de sistemas consta de las siguientes partes:

- Garantizar que la seguridad está integrada en los sistemas de información.

- Evitar errores, pérdidas, modificaciones no autorizadas o usos indebidos de la información de las aplicaciones.
- Garantizar la seguridad de los archivos del sistema.
- Mantener la seguridad del software y de la información de las aplicaciones.
- Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas.

PROTECCIÓN DE LOS SISTEMAS OPERATIVOS Y OTRAS UTILIDADES

Se prevendrá el acceso no autorizado a los sistemas operativos, así como su actualización para corregir vulnerabilidades detectadas y se proveerán de las medidas técnicas de seguridad oportunas.
Estará restringido y controlado el uso de aplicaciones no autorizadas que puedan invalidar las medidas de seguridad implantadas.

GESTIÓN DE INCIDENCIAS

Los eventos y las vulnerabilidades de la seguridad de la información asociados a los sistemas de información se comunicarán de manera que sea posible emprender las acciones correctivas oportunas.
Se aplicará un enfoque práctico, coherente y efectivo a la gestión de incidentes de seguridad de la información, recopilando las evidencias que sean necesarias.
Todos los empleados, contratistas y los terceros de Grupo Gaselec deberán notificar cualquier incidencia, o sospecha de la misma, que identifiquen, sin demora, al área de sistemas para su gestión y posterior tratamiento.

CONTINUIDAD DEL NEGOCIO

Se contrarrestarán las interrupciones de las actividades empresariales y se protegerán los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información.
Se garantizará la oportuna reanudación de todos los servicios críticos para el Grupo Gaselec.

CUMPLIMIENTO LEGAL

Se evitará cualquier tipo de incumplimiento de las leyes u obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad que afecten a los sistemas de información del Grupo Gaselec.