Política de Seguridad de la Información

La Dirección de CGB Informática, S.L., en adelante CGB , establece la Política de Seguridad de la Información siendo de aplicación para los procesos identificados en el Alcance del SGSI, a todos los empleados y terceras partes relacionadas.

Los departamentos deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS) para los requisitos de seguridad ALTA, así como la norma UNE-ISO/IEC 27001:2017. La entidad debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con los principios básicos y los requisitos mínimos indicados para el ENS (RD 3/2010).

La Dirección concretará los Objetivos de seguridad de CGB anualmente en la Revisión del Sistema. Al fijar dichos objetivos, se establecerán los responsables (seguridad como función diferenciada), los medios y acciones necesarias a realizar para poder alcanzar los mismos.

Es responsabilidad de todos, la implantación y el seguimiento de la política de seguridad, comenzando por la Dirección, que marcará los criterios estratégicos a seguir.

El SGSI establece como objetivos generales los siguientes:

- Gestionar las principales dimensiones de seguridad de la información: Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad.
- Cumplir con las necesidades y expectativas de las partes interesadas involucradas dentro del alcance del SGSI, preservando la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la información.
- Articular la seguridad como un proceso integral de todos sus elementos y aplicando una estrategia de protección por múltiples capas de seguridad.
- Demostrar liderazgo por parte de la dirección asegurando que la política de Seguridad de la Información, y los objetivos de seguridad se establecen y son compatibles con la dirección estratégica de la organización.
- Servicios con un nivel de seguridad de la información que satisfagan y superen las necesidades de nuestros clientes.
- Prevención de posibles defectos y posibles incidentes de seguridad de la información antes de que ocurran, trabajando orientados hacia la “mejora continua” y la comunicación.
- Asegurar el cumplimiento de la legislación, reglamentación y normativas aplicables, así como todos aquellos requisitos que la organización considere oportunos
- Asignación eficaz de funciones y responsabilidades en el ámbito de la seguridad.
- Revisiones continuas del Sistema de Gestión de Seguridad de la Información.
- Establecimiento de indicadores de seguridad que nos permitan conocer el grado de seguridad de nuestros procesos productivos.
- Fomento de la formación del personal de la organización en los aspectos débiles que se detecten a lo largo del ejercicio.
- Realización de auditorías de seguridad periódicas para conocer el grado de cumplimiento de la política de seguridad.
- Concienciación y motivación del personal sobre la importancia de una correcta gestión de la seguridad de la información.
- Analizar los riesgos a los que está expuesta la Organización, y gestionarlos de la mejor forma posible para alcanzar el nivel de riesgo aceptado por la Dirección y establecer el nivel de seguridad basado además en objetivos. El SGSI proporciona los mecanismos para, basándose en la metodología MAGERIT , analizar y gestionar el riesgo.

El alcance del SGSI queda definido como:

Los sistemas de información para la prestación de servicios de cloud computing, consultoría, integración y explotación de sistemas e infraestructuras informáticos, outsourcing de sistemas de información, ciberseguridad, análisis y explotación de datos y servicios de transformación digital, DE ACUERDO A LA DECLARACIÓN DE APLICABILIDAD VIGENTE.

Fecha: septiembre 2022

Carlos González. Director