Política General de Seguridad

CESCE basa su actividad en el tratamiento de diferentes tipos de datos e información, ello le permite ejecutar procesos básicos propios del negocio. Los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyen el activo principal de CESCE, de tal manera que el daño o pérdida de los mismos inciden en la realización de sus operaciones y pueden poner en peligro la continuidad de la organización.

Para que esto no suceda se ha diseñado una Política de Seguridad de la Información cuyos fines principales son:

- **Proteger**, mediante controles/medidas, **los activos** frente a amenazas que puedan derivar en incidentes de seguridad.
- **Paliar** los efectos de **los incidentes** de seguridad.
- **Establecer** un sistema de **clasificación de la información** y los datos con el fin de proteger los activos críticos de información.
- **Definir las responsabilidades** en materia de seguridad de la información generando la estructura organizativa correspondiente.
- **Elaborar** un conjunto de **reglas, estándares y procedimientos** aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
- **Especificar** los efectos que conlleva el **incumplimiento** de la Política de Seguridad en el ámbito laboral.
- **Evaluar los riesgos** que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
- **Verificar** el funcionamiento de **las medidas/controles de seguridad** mediante auditorías de seguridad internas realizadas por auditores independientes.
- **Formar a los usuarios en la gestión de la seguridad** y en tecnologías de la información y las comunicaciones.
- **Proteger a las personas** en caso de catástrofes naturales, incendios, inundaciones, ataques terroristas, etc., mediante planes de emergencia.
- **Controlar el tráfico de información y de datos** a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- **Observar y cumplir la legislación** en materia de protección de datos, propiedad intelectual, laboral, penal, etc., que afecte a los activos de CESCE.
- **Garantizar un servicio eficiente a nuestros clientes** con un alto nivel de calidad, preservando así su confianza.
- **Proteger el capital intelectual de la organización** para que no se divulgue ni se utilice ilícitamente.
- **Obtener las evidencias** que permitan acreditar los incidentes de seguridad y la identificación de su autor.

- **Reducir** las posibilidades de **indisponibilidad** a través del uso adecuado de los activos de la organización.
- **Defender los activos** ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- **Controlar el funcionamiento de las medidas de seguridad** averiguando el número de incidencias, su naturaleza y efectos.

Las distintas áreas bajo cuya responsabilidad se encuentran los servicios prestados deberán contemplar la seguridad desde el mismo momento en que se concibe un nuevo sistema o servicio, aplicando para estos y para los ya existentes, las medidas de seguridad necesarias para garantizar la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad de los servicios y de la información.

Los requisitos de seguridad de los sistemas, las necesidades de formación de los usuarios, administradores y operadores y las necesidades de financiación deben ser identificados e incluidos en la planificación de los sistemas y en los pliegos de prescripciones utilizados para la realización de proyectos que involucren a las TIC.

Se deben articular mecanismos de prevención, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad.

En cuanto a la prevención, se debe evitar que los servicios y la información resulten afectados por un incidente de seguridad. Para ello, CESCE implementará las medidas de seguridad que les son de aplicación en base a las normativas y regulaciones que afectan a su actividad, así como las medidas adicionales necesarias para contrarrestar las amenazas identificadas en el proceso de análisis de riesgos.

En cuanto a la reacción, se establecerán mecanismos de detección, comunicación y gestión de incidentes de seguridad, de forma que cualquier incidente pueda ser tratado en el menor plazo posible. Siempre que sea posible, se detectarán de forma automática los incidentes de seguridad, utilizando elementos de monitorización de los servicios o de detección de anomalías y poniendo en marcha los procedimientos de respuesta al incidente en el menor plazo posible. Para los incidentes detectados por los usuarios, ya sean internos o externos, se establecerán los pertinentes canales de comunicación de incidentes.

En cuanto a la recuperación, para aquellos servicios que se consideren críticos, en base a la valoración que de los mismos realicen sus responsables, se deberán desarrollar planes que permitan la continuidad de dichos servicios en el caso de que, a raíz de un incidente de seguridad, quedaran indisponibles.

Madrid, 17 de julio de 2023