POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Raquel García Serna

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

Como Objetivos prioritarios se deberá	• Garantizar un servicio eficiente a nuestros clientes, con un alto nivel de calidad y seguridad, preservando sus derechos y su confianza. • Proteger el capital intelectual de la Organización para que no se divulgue ni se utilice ilícitamente
Para que esto no suceda se ha diseñado la Política de Seguridad de la Información cuyos principios y objetivos son:	• La información, tanto interna como la de nuestro cliente, tiene un valor estratégico para el negocio, por lo que se debe proteger contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra. • La fuente de origen de la información debe ser fiable. La credibilidad de la información viene determinada por la autenticidad de la fuente. • La información debe estar disponible, permitiendo su acceso autorizado siempre que sea necesario. • La protección de la información se llevará a cabo mediante la aplicación de medidas de control sobre los activos que la mantienen o tratan: las personas, los soportes, las instalaciones, las comunicaciones, los sistemas, las aplicaciones, etc. Estas medidas deberán ser proporcionales al valor del activo a proteger. Los controles de seguridad aplicados nunca superarán el coste de los activos a que se aplican o el daño que en ellos se pudiese producir debido a la falta de los mismos. • Cualquier medio técnico u organizativo capaz de salvaguardar la información debe estar coordinado y alineado con el negocio. • La seguridad de la información no es sólo un acto interno, por lo que se debe obtener un compromiso formal de los proveedores y colaboradores respecto a la gestión de seguridad de la información. • La seguridad de la información es responsabilidad de todos. Todo usuario tiene la obligación de atender los requisitos impuestos y atender y comunicar cualquier indicio que pueda comprometerla. • Se debe asegurar la continuidad de las operaciones críticas para el negocio. • Los requisitos de seguridad y su cumplimiento deben de revisarse y verificarse periódicamente. • El tratamiento de la información y medidas de seguridad aplicadas deben estar siempre alineadas con las leyes, normativas y regulaciones aplicables.

	•
Para el cumplimiento de estos principios y objetivos de la seguridad de la información se deberá:	• Definir las responsabilidades en materia de seguridad de la información generando la estructura organizativa correspondiente. • Establecer un sistema de clasificación de la información y los datos con el fin de proteger los activos críticos de información. • Elaborar un conjunto de reglas, estándares, normas y/o procedimientos aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, activos de la organización, y operaciones sobre los mismos, 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, de acuerdo con la metodología y criterios de análisis y gestión del riesgo adoptada en la organización, según el documento **"RIE/AR-01 Metodología Análisis y Gestión de los Riesgos".** • Proteger, mediante controles/medidas, los activos frente a amenazas que puedan derivar en incidentes de seguridad. • Paliar los efectos de los incidentes de seguridad la mayor celeridad posible, para minimizar sus efectos y obtener las evidencias que permitan acreditar los incidentes de seguridad y la identificación de su autor. • 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. • Controlar y registrar los accesos lógico y físico a la información y sistemas asociados y la identificación de aquellos que acceden. • Verificar el funcionamiento de las medidas/controles de seguridad mediante auditorías de seguridad internas realizadas por auditores independientes. • Controlar el funcionamiento de las medidas de seguridad averiguando el número de incidencias, su naturaleza y efectos. • 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. • Observar la legislación en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc., que afecte a los activos de la Organización. • Reducir las posibilidades de indisponibilidad a través del uso adecuado de los activos de la Organización.

En Torrelavega, a 26 de agosto de 2024

Dirección de RALSET SEGURIDAD S.L.

20202910D DAVID VERDEJA (R: B39752589)

Firmado digitalmente por 20202910D DAVID VERDEJA (R: B39752589)
Fecha: 2024.08.26 12:13:50 +02'00'