Política de Seguridad de la información

En KARPAY somos conscientes de que la seguridad de la información relativa a nuestros clientes es un recurso con gran valor y que gestionamos el tratamiento de diferentes tipos de datos e información que nos permite ejecutar procesos básicos propios de nuestro negocio. Los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyen un activo importante de **KARPAY**, de tal manera que el daño o pérdida de los mismos inciden en la realización de nuestras operaciones y pueden poner en peligro la continuidad de **KARPAY**. Para que esto no suceda, hemos diseñado esta Política de Seguridad de la Información cuyos fines principales son:

- Garantizar el cumplimiento desde el punto de vista legal, ya sea ley criminal, civil, estatutaria, regulatoria o contractual.
- Definir las responsabilidades en materia de seguridad de la información generando la estructura organizativa correspondiente.
- Asegurar la confidencialidad de los datos gestionados por KARPAY.
- Proteger, mediante controles/medidas, los activos frente a amenazas que puedan derivar en incidentes de seguridad.
- Garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos necesarios para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.
- Proteger la información durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción.
- Evaluar los riesgos que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
- Reducir las posibilidades de indisponibilidad a través del uso adecuado de los activos de KARPAY.
- Defender los activos ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- Asegurar la capacidad de respuesta ante situaciones de emergencia, restableciendo el funcionamiento de los servicios críticos en el menor tiempo posible.
- Promover la concienciación y formación en seguridad de la información.
- Garantizar la seguridad de los sistemas de información y extremar las precauciones de las conexiones y accesos desde fuera del entorno habitual de trabajo, por ejemplo, en caso de teletrabajo, protegiendo los dispositivos con diferentes herramientas que aumenten su seguridad, así como las comunicaciones de acceso a la información a través de la conexión a la VPN de KARPAY instalada en los mismos.

Esta Política está implantada, mantenida al día, revisada anualmente y comunicada a todos los empleados.

LA DIRECCIÓN

21/02/23