Política de Seguridad de la Información

Con el objetivo de garantizar la protección de la Compañía desde todos sus puntos de vista es necesario proteger convenientemente nuestros activos, gestionando de forma adecuada la seguridad corporativa y maximizando la **integridad, confidencialidad y disponibilidad** de todos los elementos necesarios para el correcto funcionamiento de **Homeserve** (clientes, información, procesos, infraestructuras, personas, etc.), protegiéndolos de posibles amenazas, minimizando sus riesgos, maximizando el retorno sobre las inversiones y las oportunidades y garantizando la continuidad de sus procesos de negocio.

En relación a los activos de **Homeserve**, consideramos especialmente relevante para nuestro negocio la protección de la información corporativa y de los elementos que la tratan, activos sin duda críticos para nosotros y nuestra Compañía y que deben mantenerse razonablemente a salvo de cualquier amenaza que pueda suponer un riesgo para ellos. La seguridad de la información debe garantizarse sin detrimento de la protección de otros elementos de nuestra Compañía, y atendiendo en todo momento a los principios legales, organizativos y técnicos correspondientes. De esta forma, **todos y cada uno de nosotros debemos conocer y cumplir la política de seguridad definida y los procedimientos, normativas, estándares y recomendaciones que la desarrollan** y pueden afectar a nuestras tareas dentro de la **compañía**. En esta línea la Dirección de **Homeserve** establece un **compromiso público** para garantizar los niveles de protección adecuados a los requisitos de la Compañía, poniendo a disposición del personal de la Compañía todos los medios necesarios para lograr este objetivo. Asimismo, se manifiesta el compromiso de mejora continua del sistema de gestión de la seguridad de la información.

Con el fin de garantizar la protección efectiva de los recursos corporativos necesarios para el correcto funcionamiento de la Compañía, tanto de amenazas externas como, se establecen los principios básicos de la Política de Seguridad de **Homeserve,** que se enumeran a continuación:

1. Cumplir los requisitos legales y contractuales aplicables al desarrollo de sus funciones en la Compañía, en especial, y a efectos de la presente política, en las materias relacionadas con la protección de datos de carácter personal y con la continuidad de los procesos de negocio.
2. Todo el personal de **Homeserve** debe conocer, cumplir y hacer cumplir procesos o procedimientos aplicables en materia de seguridad de la información, individualmente en función de sus tareas dentro de la Compañía.
3. Restringir el uso tanto de la información en sí como de los sistemas que la procesan, que son propiedad de **Homeserve**, a aquellas tareas necesarias para el correcto desempeño del trabajo de cada persona dentro de las Compañías; sin estar permitido el uso en beneficio particular de ningún activo.
4. En el caso de la información, considerada como uno de los activos principales de **Homeserve** y que pertenece a cada Compañía, es deber de todo el personal mantener el secreto respecto a la misma y no divulgarla a terceros, salvo que las comunicaciones formen parte de la relación profesional.

Homeserve podrá monitorizar e investigar en caso de potencial incidente de seguridad el correcto uso de los equipos, ficheros y sistemas.

Dicho control general tendrá por finalidad verificar el cumplimiento de las obligaciones que corresponden a cada trabajador, en relación con el uso de los medios y herramientas informáticas, titularidad de **Homeserve**, y velar por la seguridad de los sistemas de información.

El trabajador, mediante la aceptación de la **Normativa uso de sistemas de información** en vigor, consiente expresamente en el control general realizado por la empresa, que se realizará siempre respetando al máximo la intimidad y dignidad del trabajador.

Cada uno de nosotros jugamos un papel fundamental en lo que a garantizar la seguridad de la información se refiere. Por este motivo, se remarcan los siguientes puntos:

- Se debe hacer un uso responsable de los recursos de la organización tales como correo electrónico, equipos de trabajo, dispositivos móviles, etc. De acuerdo con lo indicado en la normativa de uso del sistema de información (ver ***NR-A08-001 Normativa uso de sistemas de información***).

- Es muy importante proteger las credenciales de acceso al sistema de información (usuario y contraseña) y nunca se deben comunicar a terceras personas (ver ***NR-A08-001 Normativa uso de sistemas de información***).
- La información que manejamos es propiedad de Reparalia y no debe ser difundida o enviada a terceras personas, sin autorización previa de nuestro responsable inmediato (ver ***NR-A08-002 Clasificación de la información***).
- Se debe informar al personal TIC o al Responsable de Seguridad de cualquier anomalía que pudiera suponer un incidente de seguridad: robos, fugas de información, accesos no autorizados, etc. (ver ***PE-07 01 IT Gestión de Incidentes***).
- Es responsabilidad de cada empleado mantener su puesto de trabajo ordenado evitando que se produzcan accesos no autorizados a la documentación, en concordancia con la política de puesto despejado y pantalla limpia establecida (ver ***PO-A11-001 Pol puesto trabajo desp y pant limpia***).

El no cumplimiento de la presente política de seguridad, o de las directrices o legislación aplicable en cada caso, provocará la adopción de las correspondientes medidas legales, definidas por cada Compañía.

Fdo: Responsable de Seguridad

Fdo: CIO

Madrid a 1 de marzo de 2017