Política de Seguridad de la Información

Tabla de contenidos

Política de Seguridad de la Información

La información es un activo fundamental para el funcionamiento de las empresas y un bien crítico sin el cual no podría desarrollar su actividad. Grupo Codere basa en gran medida la calidad de su gestión en la utilización de su información de forma exacta, completa y obtenida a tiempo.

La Dirección del Grupo Codere reconoce su responsabilidad en desarrollar las directrices de Seguridad de la Información que permitan minimizar los riesgos potenciales a los que se encuentra expuesta en la consecución de los objetivos estratégicos del negocio.

1. Aspectos Organizativos

Grupo Codere debe definir y asignar las funciones y responsabilidades del personal del Grupo en materia de ciberseguridad para una correcta organización y desarrollo de la estrategia de la compañía. De esta forma, se garantiza la segregación de funciones y se evitan conflictos de interés.

2. Seguridad ligada a los Recursos Humanos

Las responsabilidades en materia de seguridad deben ser consideradas en el proceso de selección de personal, en la elaboración de los contratos y durante la etapa laboral, a fin de reducir los riesgos de manipulación, robo, fraude o uso inadecuado de la información.

Los términos y condiciones deben incluir aspectos como acuerdos de confidencialidad, derechos legales, responsabilidades para el cumplimiento del cuerpo normativo y para el tratamiento de información de terceros y acciones a tomar si la persona no cumple con los requisitos de seguridad.

Todo el personal de Grupo Codere debe recibir un nivel adecuado de formación y concienciación en materia de Seguridad de la Información, así como ser informados correctamente de sus labores y responsabilidades en materia de Seguridad de la Información.

3. Gestión de Activos

Grupo Codere debe establecer un conjunto de medidas para organizar los activos de información, mantener su integridad y protegerlos de fugas, borrados accidentales o accesos no autorizados.

Toda la información del Grupo debe clasificarse para facilitar los procesos de control de acceso, custodia y monitorización. En base al nivel de clasificación de la información establecido, el Grupo debe establecer medidas y controles preventivos, y cuanto más confidencial se considere la información, más restrictivos deben ser dichos controles.

4. Control de Accesos

El acceso por parte del personal interno o externo a los sistemas de información de Grupo Codere, así como a la información que tratan o almacenan, se debe regular sobre la base de las necesidades de información y operación de cada usuario, otorgando acceso exclusivamente a aquellas funciones e información que se requieran para el correcto desempeño de su actividad laboral, acorde con su función y/o perfil operacional.

Todos los accesos realizados por los usuarios a los sistemas de información de Grupo Codere, deben llevar asociado un proceso de identificación, autenticación y autorización, estableciéndose los controles adecuados para que tales procesos se realicen de forma segura. Se deben diseñar e implantar mecanismos de registro, monitorización de acceso y uso de los sistemas, que permitan conocer la efectividad de las medidas instaladas y detectar posibles incidentes de Seguridad.

5. Controles Criptográficos

Grupo Codere debe aplicar controles criptográficos en base a la necesidad de implantar dichos controles en función del nivel de seguridad requerido por la tipología de información existente en los diferentes entornos y plataformas para garantizar la confidencialidad de la información.

Los métodos de cifrado utilizados en Grupo Codere deben estar reconocidos como no vulnerables por las buenas prácticas de Seguridad. Toda información sensible, confidencial y de carácter personal debe estar cifrada.

Las claves de cifrado deben ser almacenadas en aquellos sistemas corporativos destinados a dicho fin, deben ser adecuadamente protegidas y el acceso a las mismas solo debe estar permitido a través de un proceso estricto de autorización con el fin de preservar su confidencialidad. Del mismo modo, se debe definir el periodo de vida de las claves de cifrado en el momento de su creación.

6. Seguridad física y Ambiental

Los espacios físicos donde se ubican los sistemas de información y los destinados al ámbito laboral de Grupo Codere deben estar adecuadamente protegidos mediante controles de acceso perimetrales, sistemas de video vigilancia y medidas preventivas de accidentes ambientales de manera que pueden evitarse incidentes de seguridad y accidentes ambientales.

El Grupo debe establecer medidas de seguridad para proteger los activos físicos dentro y fuera del entorno laboral. Es necesario disponer de normas de mesas limpias para proteger la información en papel.

7. Seguridad en la Operativa

Todos los sistemas de información del Grupo Codere deben contar con soluciones actualizadas que impidan que el funcionamiento de los equipos y aplicaciones pueda verse afectado por las acciones dañinas de softwares maliciosos. Se deben realizar distintas prácticas de prevención, detección y eliminación de elementos perjudiciales, que deben formalizarse y especificarse en una norma propia.

Adicionalmente, todos los sistemas deben de ser analizados para la identificación y mitigación de sus vulnerabilidades y ningún sistema en el entorno de producción debe de estar fuera del ciclo de vida de soporte por los fabricantes ni debe estar activo si se ha detectado una vulnerabilidad crítica en él.

Además, toda actividad debe ser registrada y monitorizada por los dispositivos de seguridad y se deberá centralizar en los sistemas de registros de eventos, correlación y monitorización.

8. Seguridad en las Telecomunicaciones

La información transmitida por redes de comunicaciones, públicas o privadas, debe ser adecuadamente protegida mediante mecanismos de seguridad que garanticen su confidencialidad, disponibilidad e integridad. Se deben establecer los controles necesarios que impiden la suplantación del emisor, modificación o pérdida de la información transmitida, tanto en las comunicaciones con sistemas situados en las redes internas, como con entidades con las que Grupo Codere tenga relación.

9. Seguridad en Proveedores

Se debe prestar especial atención en evaluar la criticidad de todos los servicios susceptibles de ser subcontratados de manera que puedan identificarse aquellos que sean relevantes desde el punto de vista de la Seguridad de la Información, ya sea por su naturaleza, la sensibilidad de los datos que deban tratarse o la dependencia sobre la continuidad del negocio.

Sobre los proveedores de estos servicios se cuidarán los procesos de selección, requerimientos contractuales, la monitorización de los niveles de servicio y las medidas de Seguridad implantadas por dicho proveedor.

10. Gestión de Incidentes

Grupo Codere debe disponer de un proceso de respuesta ante incidentes para gestionar de forma correcta todas las amenazas materializadas en el Grupo. Este proceso incluye aspectos como la monitorización, seguimiento, clasificación y remediación de dichos incidentes.

Todo incidente que pueda comprometer o haya comprometido la confidencialidad, integridad y/o disponibilidad de la información debe ser registrado y analizado para aplicar las correspondientes medidas correctivas y/o preventivas.

Todo empleado y colaborador externo al Grupo tiene la obligación y responsabilidad de notificar a los responsables de seguridad de cualquier sospecha, incidente o delito que pueda comprometer la seguridad de los activos de información del Grupo.

11. Continuidad de Negocio

Se debe disponer de un plan de continuidad de negocio como parte de la estrategia del Grupo, para garantizar la continuidad en la prestación de sus servicios vitales y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para que la organización actúe en caso de ser necesario.

El plan de contingencia se debe desarrollar e implementar para asegurar que los procesos críticos de negocio puedan restablecerse en el tiempo requerido, incluyendo controles para identificar y reducir los riesgos, limitar las consecuencias de los incidentes que afectan negativamente, y asegurar el tiempo de respuesta de las operaciones esenciales.

12. Cumplimiento Normativo y Legal

Grupo Codere debe cumplir con todos aquellos requerimientos legales, regulatorios y contractuales que le sean de aplicación. Es fundamental formalizar un marco de control asociado al Cuerpo Normativo de Seguridad para verificar y realizar un seguimiento de su cumplimiento.