

Reglamento de seguridad de la información de Future Concept SAC

Introducción

Este reglamento tiene como objetivo establecer las medidas y acciones necesarias para garantizar la protección de la información y los activos relacionados de Future Concept SAC contra el acceso no autorizado, el uso indebido, la divulgación y la alteración. Este reglamento se basa en la política de seguridad de la información de Future Concept SAC y se aplica a todas las áreas de negocio, empleados, contratistas, proveedores y terceros que interactúen con la organización.

Identificación de los activos de información

Future Concept SAC identificará y documentará todos los activos de información relevantes y sus propietarios. La clasificación de la información se basará en su importancia, su sensibilidad y su nivel de riesgo. Los activos de información se etiquetarán con una clasificación adecuada y se establecerán controles de acceso adecuados.

Acceso a la información

El acceso a la información se limitará a aquellos que necesiten tener acceso para realizar sus funciones y responsabilidades. Los derechos de acceso se otorgarán de acuerdo con la necesidad de conocer la información para realizar las tareas relacionadas con el trabajo. El acceso se revocará cuando ya no sea necesario o cuando se produzca una violación de la seguridad de la información.

Política de contraseñas

Future Concept SAC establecerá una política de contraseñas que incluya la complejidad de las contraseñas, la periodicidad de cambio, la prohibición de reutilización de contraseñas, la necesidad de contraseñas seguras en los sistemas críticos y la limitación del número de intentos de inicio de sesión.

Protección de los activos de información

Future Concept SAC establecerá controles de seguridad adecuados para proteger los activos de información contra la pérdida, la destrucción, la corrupción, el robo o el daño. Estos controles incluirán medidas de seguridad físicas, técnicas y organizativas apropiadas para la clasificación y el nivel de riesgo de los activos de información.

Política de seguridad de la red

Future Concept SAC establecerá una política de seguridad de la red que incluya la protección de la red contra ataques malintencionados y la gestión de la seguridad de los dispositivos de red. Los dispositivos de red se configurarán de acuerdo con las mejores prácticas de seguridad y se actualizarán regularmente para protegerlos contra vulnerabilidades conocidas.

Gestión de incidentes de seguridad de la información

Future Concept SAC establecerá y mantendrá un proceso para informar, investigar y responder a los incidentes de seguridad de la información. Todos los incidentes de seguridad de la información se notificarán a la persona responsable del sistema de gestión de seguridad de la información (SGSI) de Future Concept SAC. Se tomarán medidas para evitar la recurrencia de los incidentes de seguridad de la información.

Uso de dispositivos móviles

Todo empleado que use un dispositivo móvil (como un teléfono inteligente, una tableta o una computadora portátil) para acceder a la información de Future Concept SAC debe proteger el dispositivo con una contraseña segura y cifrado de datos. Los dispositivos móviles deben mantenerse actualizados con los últimos parches y actualizaciones de seguridad. Los empleados deben informar inmediatamente si pierden o les roban un dispositivo móvil que contenga información de Future Concept SAC.

Copias de seguridad y restauración

Future Concept SAC realizará regularmente copias de seguridad de la información y los sistemas para garantizar la recuperación en caso de interrupciones o desastres. Los empleados deben seguir las políticas y procedimientos de copia de seguridad y restauración para garantizar la integridad y disponibilidad de la información.

Análisis y monitoreo

Future Concept SAC realizará regularmente análisis y monitoreo de la información y los sistemas para detectar y prevenir posibles amenazas de seguridad. Los empleados deben informar inmediatamente cualquier actividad sospechosa o inusual que puedan detectar.

Pruebas de seguridad

Future Concept SAC realizará regularmente pruebas de seguridad en los sistemas y aplicaciones para detectar posibles vulnerabilidades y garantizar la eficacia de los controles de seguridad. Los empleados deben seguir las políticas y procedimientos de pruebas de seguridad para garantizar la seguridad de la información.

Revisiones y auditorías

Future Concept SAC realizará revisiones y auditorías regulares del sistema de gestión de seguridad de la información para garantizar su efectividad y cumplimiento de las políticas y procedimientos. Los empleados deben colaborar con las revisiones y auditorías proporcionando la información y los datos necesarios.

Cumplimiento legal y contractual

Future Concept SAC cumplirá con las leyes, regulaciones y normas aplicables relacionadas con la seguridad de la información y garantizará el cumplimiento de los requisitos contractuales relacionados con la seguridad de la información. Los empleados deben seguir las políticas y procedimientos para garantizar el cumplimiento legal y contractual.

Consecuencias de incumplimiento

Future Concept SAC se reserva el derecho de tomar medidas disciplinarias, incluida la terminación del empleo, contra cualquier empleado que viole la política de seguridad de la información. Los empleados son responsables de informar cualquier violación de la política de seguridad de la información a su supervisor inmediato o al responsable del sistema de gestión de seguridad de la información.

Revisión y actualización

Future Concept SAC revisará y actualizará regularmente la política de seguridad de la información y el reglamento para garantizar su efectividad y relevancia. Los empleados deben estar al tanto de los cambios en la política y el reglamento y seguir los procedimientos actualizados.

Lima, 01 de Octubre de 2022



+51 992 743 849



Av. Santo Toribio 143, 2do piso – Oficina 55
San Isidro, Lima – Perú



innovacion@futurelab.pe

www.futurelab.la

