SCMP

Supply Chain Management Perú SAC

POLÍTICA DE CIBERSEGURIDAD Y TECNOLOGÍA DE LA INFORMACIÓN

SUPPLY CHAIN MANAGEMENT PERÚ SAC es una empresa que realiza el servicio de Supervisión de ruta, escolta de convoy, Centro de Control, Check Point y Respuesta a Emergencias en el sector Industrial y Minero.

SUPPLY CHAIN MANAGEMENT PERÚ SAC ha resuelto establecer una Política de Ciberseguridad y Tecnología de la Información, la cual tiene como objetivo gestionar el riesgo y el rol en la cadena de suministro.

Por ello, asumimos los siguientes compromisos:

1. Establecer, documentar y mantener criterios de seguridad que permitan identificar y proteger los sistemas de las tecnologías de la información y recuperarla oportunamente en caso de ser necesario.
2. Identificar partes interesadas y su nivel de criticidad en la infraestructura informática (hardware y software) de la empresa.
3. Comunicar oportunamente información sobre amenazas de ciberseguridad identificadas a las partes interesadas correspondientes.
4. Clasificar la información de acuerdo con la legislación vigente, sistemas y accesos según el nivel de criticidad y establecer políticas de acceso a la misma.
5. Utilizar cuentas asignadas para cada usuario que acceda al sistema, con sus propias credenciales de acceso mediante contraseñas u otras formas de autenticación que generen accesos seguros. Están deben actualizarse periódicamente, cuando existan indicios o sospechas razonables de que están comprometidas.
6. Limitar los accesos y permisos de los usuarios de acuerdo con las funciones y tareas asignadas, revisándolos periódicamente.
7. Eliminar el acceso a la información a todos los colaboradores, terceros y usuarios externos al terminar su contrato o acuerdo.
8. Impedir la instalación de software no autorizado.
9. Utilizar y mantener hardware y software licenciados y actualizados para proteger la infraestructura de TI contra amenazas informáticas tales como virus, programas espías, gusanos, troyanos, malware, ransomware, entre otros.
10. Realizar copias de seguridad de la información sensible, manteniendo un respaldo fuera de las instalaciones (física o virtual) con las medidas de seguridad necesarias para impedir que terceros accedan a la información.
11. Mantener un registro actualizado de los usuarios, su nivel de criticidad y accesos asignados.
12. Cerrar/bloquear la sesión en equipos desatendidos.
13. Evaluar mínimo una vez al año la seguridad de la infraestructura de TI (hardware y software), implementando acciones pertinentes cuando se hayan detectado vulnerabilidades.
14. Establecer procedimientos y controles para identificar y revisar el acceso no autorizado a los sistemas de información, sitios web, o el incumplimiento de las políticas y procedimientos (incluyendo la manipulación o alteración de los datos comerciales por parte de los colaboradores o contratistas).
15. Revisar las políticas y los procedimientos de ciberseguridad al menos una vez al año y actualizarlas cuando se presenten cambios en el contexto interno o externo, o cuando se materialice algún riesgo.
16. Emplear tecnologías seguras, como redes privadas virtuales (VPN) o autenticación multifactor para el acceso seguro de los colaboradores y usuarios externo a los sistemas informáticos de la empresa, incluyendo accesos para trabajo remoto o teletrabajo.
17. Establecer procedimientos para evitar el acceso remoto de usuarios no autorizados, desde dispositivos personales u otros.
18. Controlar mediante la realización de inventarios periódicos, los medios u otros equipos que hagan parte de la infraestructura informática de la empresa. La eliminación o desecho de los mismos se hará de acuerdo con la legislación vigente.
19. Restringir la conexión de dispositivos personales y elementos periféricos no autorizados para cualquier dispositivo que forme parte de la infraestructura informática de la empresa.
20. Vigilar el cumplimiento de las políticas de ciberseguridad y seguridad de la información establecidas en el uso de plataformas y contenido digital, herramientas de videoconferencia, comercio electrónico, entre otras.
21. Realizar ejercicios prácticos y/o simulacros relacionados con la seguridad de las tecnologías de la información, que permitan determinar la eficacia de las acciones establecidas.
22. Establecer controles para super usuarios que permitan la continuidad de credenciales de los equipos activos, en caso que aplique.

Gina Erika Quijano Mori
Gerente General

Revisión: 10/04/2023
Aprobación: 19/03/2022
Versión: 01