Políticas de Seguridad de Tecnologías de la Información y Comunicación (TIC) para EMPOCABAL ESP-EICE

Introducción: Las políticas de seguridad de Tecnologías de la Información y Comunicación (TIC) de EMPOCABAL ESP-EICE tienen como objetivo establecer lineamientos y procedimientos para garantizar la integridad, confidencialidad y disponibilidad de la información, así como la protección de los activos tecnológicos de la empresa. Estas políticas se aplican a todo el personal y terceros que tengan acceso a los sistemas y datos de la organización.

1. Responsabilidad y autorización:

   1.1. Se asignarán responsabilidades claras sobre la gestión y el cumplimiento de la seguridad TIC a través de roles y funciones designadas.

   1.2. Se establecerá un proceso formal para autorizar y revocar los accesos a los sistemas y datos de acuerdo con los principios de menor privilegio y necesidad de conocer.

2. Protección de datos y confidencialidad:

   2.1. La información clasificada como confidencial o sensible deberá ser protegida mediante controles de acceso y cifrado, y solo deberá ser compartida con personal autorizado y con propósitos legítimos.

   2.2. Se implementarán mecanismos de control para evitar la divulgación no autorizada de información sensible, ya sea en medios digitales o físicos.

3. Uso adecuado de los recursos TIC:

   3.1. Se establecerán pautas claras sobre el uso adecuado de los recursos TIC, incluyendo equipos, software y servicios en línea, con el objetivo de prevenir el uso indebido y garantizar la productividad del personal.

   3.2. Se prohíbe expresamente el uso de los recursos TIC para actividades ilegales o que pongan en riesgo la seguridad de la organización.

4. Seguridad física:

   4.1. Se establecerán medidas de seguridad física para proteger los activos tecnológicos y la infraestructura de las instalaciones de EMPOCABAL ESP-

EICE, incluyendo el acceso restringido a áreas sensibles y la implementación de sistemas de videovigilancia cuando sea necesario.

5. Gestión de incidentes de seguridad:

   5.1. Se establecerá un procedimiento formal para la identificación, notificación y respuesta a incidentes de seguridad TIC, con el fin de mitigar sus efectos y evitar su recurrencia.

   5.2. Todo el personal deberá reportar cualquier incidente de seguridad, sospecha de brecha o comportamiento sospechoso de manera inmediata.

6. Actualizaciones y parches:

   6.1. Se mantendrán actualizados los sistemas y aplicaciones con las últimas actualizaciones y parches de seguridad disponibles, con el fin de corregir vulnerabilidades conocidas y proteger los activos de la organización.

7. Copias de seguridad y recuperación de datos:

   7.1. Se establecerá una política de copias de seguridad regular y periódica de la información crítica almacenada en los sistemas de EMPOCABAL ESP-EICE.

   7.2. Se realizarán pruebas periódicas de recuperación para asegurar la integridad y disponibilidad de los datos en caso de incidentes o desastres.

8. Educación y concienciación en seguridad:

   8.1. Se llevarán a cabo programas de formación y concienciación en seguridad TIC para el personal, con el objetivo de promover buenas prácticas y reducir el riesgo de incidentes de seguridad causados por desconocimiento.

9. Cumplimiento legal y normativo:

   9.1. EMPOCABAL ESP-EICE cumplirá con todas las leyes y regulaciones aplicables relacionadas con la seguridad y protección de la información y los datos personales.

10. Revisión y actualización de políticas:

10.1. Estas políticas de seguridad TIC serán revisadas periódicamente para garantizar su efectividad y adecuación a los cambios en el entorno tecnológico y normativo.

Es importante que estas políticas sean comunicadas a todos los empleados y colaboradores relevantes, y que se les proporcione la capacitación adecuada para garantizar su cumplimiento. Además, se debe asegurar una supervisión continua para verificar que estas políticas se están aplicando y manteniendo de manera efectiva.

Coordinación de sistemas de información
EMPOCABAL ESP EICE.