



Ciberseguridad de productos

Confidencialidad, integridad y disponibilidad
para una movilidad segura en el edificio

We Elevate



Schindler

Schindler transporta hasta

1.500.000.000.

de personas cada día.

Vivimos en un mundo conectado en el que se nos presentan desafíos globales.

La digitalización y la conectividad pueden ayudar a potenciar el valor que ofrecemos a nuestros clientes, al mismo tiempo que nos permiten desarrollar productos y servicios innovadores, para una movilidad urbana inteligente que fomente el movimiento de la sociedad. No obstante, la adopción de estas nuevas tecnologías subraya la importancia de establecer un entorno ciberresiliente.

Ciberresiliencia

Dado que los ascensores y escaleras mecánicas están cada vez más conectados y sus sistemas dependen crecientemente de información compleja en la red, la tarea de prevenir vulneraciones y proteger la información se ha convertido en una prioridad absoluta, para maximizar el tiempo de actividad y la disponibilidad de nuestros sistemas.

Cuando nos centramos en la ciberseguridad, el primer paso es analizar la tríada de la confidencialidad, la integridad y la disponibilidad (CIA, por sus siglas en inglés): un reconocido modelo para el desarrollo de la ciberseguridad. Estos conceptos sirven de guía al afrontar las actividades del proceso de desarrollo.

La **confidencialidad** garantiza que quienes no estén autorizados no puedan acceder a los datos intercambiados.

La **integridad** es la capacidad de garantizar que un sistema y sus datos no han sufrido ninguna modificación no autorizada, y que son correctos y completos.

La **disponibilidad** garantiza que los sistemas, aplicaciones y datos estén a disposición de los usuarios cuando los necesiten.

Movilidad segura. Confidencialidad de los datos

Ciberseguridad para los productos conectados

Actuamos rápido

Todos los productos de Schindler deben pasar por una estricta evaluación de seguridad informática de productos durante su desarrollo. Expertos externos e internos se aseguran de que los últimos estándares se cumplan en todo momento. Nuestro equipo de arquitectura de sistemas, se encuentra en mejora constante con la revisión periódica de los procesos de datos y la gestión de certificados.

- Evaluación y aplicación de los últimos protocolos, certificados y diseño para un funcionamiento y protección fiables.
- Supervisión remota de las unidades conectadas con principios de autenticación y autorización restringidos.
- El motor de reglas de Schindler supervisa los datos entrantes según su coherencia.
- Evaluaciones de seguridad y actualizaciones frecuentes para las aplicaciones.

Los ascensores y escaleras mecánicas de Schindler han evolucionado hasta convertirse en sistemas inteligentes y conectados, que permiten su supervisión remota y la conexión con las aplicaciones móviles de los usuarios. Innovamos para que la gente se siga moviendo de forma segura y cómoda. En el núcleo de esta cultura de innovación reside la ciberresiliencia y una mentalidad donde prima la seguridad. Juntos nos adaptamos sin descanso a unas ciberamenazas que nunca dejan de avanzar.

Seguridad de productos

Los productos de Schindler son cada vez más capaces de interactuar e intercambiar datos gracias a la electrónica integrada, al software, sensores, conectividad y electrónica integrados. El objetivo de Schindler es minimizar el riesgo y la exposición de sus productos conectados a las amenazas de seguridad garantizando la protección de los mismos a lo largo de todo el ciclo de vida. Los principios de seguridad están integrados en nuestras fases de diseño y desarrollo del producto y, además, se llevan a cabo análisis de vulnerabilidad.

Ciberresiliencia

Schindler diseña e implementa prácticas y capacidades ciberresilientes en toda la organización, incluida la administración de la continuidad empresarial, para promover la disponibilidad de los servicios y aplicaciones de la empresa mientras garantiza la confidencialidad de los datos. Además, los vanguardistas servicios informáticos de supervisión de la seguridad son capaces de identificar riesgos cibernéticos potenciales.

Objetivo: una movilidad conectada y segura de extremo a extremo

Nuestros dispositivos que conectan los ascensores y andenes móviles a través de Internet están protegidos frente a accesos no autorizados, y el sistema está respaldado mediante componentes de seguridad electromecánicos.

- Gestión de certificados para una comunicación M2M.
- Interfaz y sistema operativo reforzados.
- Software y aplicaciones de Schindler especiales y seguras en la pasarela de comunicación.

Supervisamos de forma constante

Supervisamos el estado y el funcionamiento, para garantizar la máxima disponibilidad y seguridad. Toda la comunicación está cifrada de extremo a extremo. Los datos críticos solo se comparten con el personal autorizado, para llevar a cabo el mantenimiento remoto o *in situ*.

- Autenticación multifactor para la gestión de dispositivos y usuarios.
- Comunicación cifrada íntegramente.
- Comunicación basada en certificados entre entidades y dispositivos.

Procesos estándar. Diversos desafíos

Seguridad desde el diseño: una filosofía y una promesa

Las actualizaciones de software frecuentes, la supervisión del funcionamiento de la red y el sistema, la programación de copias de seguridad y el cifrado de los archivos y carpetas son requisitos fundamentales de nuestra promesa de seguridad desde el diseño. Los mecanismos de prevención de pérdida de datos, el control de los dispositivos y la creación de listas blancas ofrecen capas adicionales de protección frente a los posibles daños causados por el malware.

Nuestra filosofía no consiste meramente en proteger nuestros equipos, redes, comunicaciones y datos, sino todo el ecosistema en el que opera nuestra tecnología.

¿El resultado final? Los ascensores Schindler pueden trasladar a sus usuarios con total confianza. Los dueños de los edificios tienen la certeza de que sus sistemas de transporte vertical son seguros.

“
Innovamos para que la gente se siga moviendo de forma segura y cómoda. En el núcleo de esta cultura de innovación reside la ciberresiliencia y una mentalidad, donde prima la seguridad.
”



Formación

La formación frecuente para la concienciación sobre ciberseguridad advierte a los empleados de los riesgos de seguridad. La formación avanzada para expertos garantiza la obtención de conocimientos exhaustivos sobre seguridad.

Requisitos

Los requisitos de seguridad vienen especificados, se revisan y están basados en el modelo de amenazas, la normativa y las políticas de seguridad.

Diseño

La arquitectura del sistema y los componentes se diseñan y revisan, para cumplir los requisitos de seguridad y garantizar la existencia de múltiples capas de defensa.

Implementación

El software se implementa y revisa de acuerdo con las normas y prácticas recomendadas en materia de codificación segura.

Verificación

El sistema y los componentes se verifican para asegurarse que todos los requisitos de seguridad estén correctamente implementados. Se realizan auditorías independientes con pruebas de penetración para garantizar la seguridad.

Lanzamiento

Los productos sólo se comercializan tras su correcta verificación e incluyen documentación del usuario, donde se recogen directrices para una configuración, instalación, funcionamiento y mantenimiento seguros.

Funcionamiento

El funcionamiento seguro se garantiza a través de la gestión de actualizaciones de software y el seguimiento de las directrices de seguridad.

Supervisión

Los sistemas están sometidos a una supervisión constante para detectar anomalías y evitar problemas de seguridad.



Soluciones digitales de un solo socio

Movilidad urbana inteligente para ascensores y escaleras mecánicas con servicios impulsados por datos

Schindler es un socio de confianza en el camino hacia la digitalización. Con un creciente ecosistema de aplicaciones y soluciones, los ascensores y escaleras mecánicas, pueden aportar mayor comodidad y confort a los pasajeros, aumentar la eficiencia y fiabilidad de la movilidad, y aportar más valor a los edificios en los que se encuentran.