Medidas Técnicas y Organizativas

Aplicaciones en la nube de control de acceso

1 ALCANCE

Las medidas técnicas y organizativas que se describen a continuación se aplican a las plataformas en la nube de control de acceso de SALTO a las que se refieren estas medidas técnicas y organizativas en su contrato de tratamiento de datos aplicable.

SALTO reserves the right to modify and update these measures at any time without notice as long as we maintain a comparable or better level of security.

2. LISTA DE MEDIDAS TÉCNICAS Y ORGANIZATIVAS

A continuación puede encontrar la lista de medidas de seguridad aplicadas por SALTO:

- Políticas de seguridad: SALTO implementa políticas y estándares de seguridad de obligado cumplimiento en toda la organización. Las políticas de seguridad se revisan periódicamente y se actualizan si es necesario para mitigar la exposición al riesgo y mantener las plataformas y los datos seguros.
- Conciencia de seguridad: SALTO realiza periódicamente campañas de sensibilización en toda la organización para prevenir y mitigar los riesgos de los usuarios.
- Seguridad física: SALTO protege sus instalaciones utilizando los sistemas de control de acceso adecuados (pe cerraduras de puertas inteligentes) para restringir el acceso al personal autorizado. Además, las áreas seguras como los centros de datos cuentan con medidas de protección adicionales contra las amenazas ambientales. Para garantizar el correcto funcionamiento, las medidas de protección (climatización, extinción de incendios, etc.) se someten a un mantenimiento periódico. Además, SALTO utiliza proveedores de colocación de terceros de confianza que también incorporan controles de seguridad físicos de conformidad con los estándares de la industria.
- Incidentes de seguridad: SALTO mantiene planes de respuesta a incidentes que incluyen la gestión de violaciones de datos personales.
- Control de accesos: SALTO implements appropriate access control to ensure access to the applications and systems in general is restricted according to least privilege and need to know principles. All personnel access SALTO's systems with a unique identifier (user ID). In case personnel leaves the company, their access rights are revoked.
- Seguridad de la red: SALTO emplea conexiones encriptadas y autenticadas para conectarse a plataformas y sistemas en general utilizando capacidades de seguridad como firewalls, VPN, mecanismos de autenticación, etc.
- Estaciones de trabajo seguras: SALTO implementa la protección adecuada sobre los dispositivos del usuario final, como protección antimalware avanzada, cifrado del disco duro y niveles de parches apropiados.
- Privacidad y seguridad por diseño: SALTO aplica los principios de privacidad y seguridad desde el diseño al adoptar un nuevo sistema o mejorar uno existente.
- Gestión de vulnerabilidades: SALTO realiza revisiones de seguridad periódicamente y corrige las vulnerabilidades

identificadas para mantener las plataformas seguras.

- Resistencia: SALTO adopta planes de respaldo y recuperación ante desastres para situaciones adversas.
- Garantía: SALTO realiza revisiones periódicas para asegurar el cumplimiento de las políticas y estándares de seguridad.

Descargo de responsabilidad: