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 se reserva el derecho de modificar y actualizar estas medidas en cualquier momento sin previo aviso siempre que mantengamos un nivel de seguridad comparable o superior.

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 (p. e., 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 acceso: Salto implementa un control de acceso adecuado para garantizar que el acceso a las aplicaciones y sistemas en general esté restringido de acuerdo con los principios de privilegio mínimo y necesidad de saber. Todo el personal accede a los sistemas de Salto con un identificador único (ID de usuario). En caso de que el personal abandone la empresa, se revocan sus derechos de acceso.
- Seguridad de red: Salto emplea conexiones encriptadas y autenticadas para conectarse a plataformas y sistemas en general utilizando funciones 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.

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

Disclaimer: