Soporte del sistema. Cuando te haga falta.

Introducción
Siemens ofrece servicios de soporte remoto utilizando una conexión remota segura hasta un sistema del cliente. Al ofrecer un servicio proactivo y más rápido, aseguramos una disponibilidad del sistema más alta.

Desde el principio, hemos asignado la más alta prioridad a la seguridad de los datos y a la protección del acceso. Nuestro concepto de la seguridad se divide en dos partes. La primera es sobre el componente operacional general y explicará el concepto básico de Siemens Remote Service (SRS), nuestro soporte del servicio en cuanto a procesos y aplicaciones además de las capacidades técnicas de nuestros productos. Está destinado principalmente a aquellos administradores de TI y directores técnicos interesados en obtener un entendimiento básico de cómo funciona SRS y lo que hacemos para asegurar y mantener la privacidad de los datos. En la segunda parte, hablamos sobre el concepto técnico y organizativo. Aquí los especialistas en TI y los expertos en seguridad de datos aprenden en detalle sobre las medidas de seguridad técnicas y organizativas que tomamos para conseguir un alto nivel de seguridad y privacidad de datos del sistema. También explicaremos cómo se establece una conexión a través de nuestra plataforma SRS, el aspecto que ofrece nuestra infraestructura de seguridad y lo que hacemos para prevenir ataques maliciosos. Este documento también ofrece un resumen general de medidas relacionadas con la seguridad TI que SRS ofrece.

Ventajas de SRS
El servicio remoto proporciona soporte adicional para dar un servicio óptimo a tus sistemas de seguridad contra incendios, seguridad y automatización de edificios ante una complejidad cada vez mayor.

He aquí las ventajas principales de SRS:
- Monitorización remota para detectar y corregir proactivamente interrupciones, al objeto de minimizar los tiempos de inactividad de los sistemas.
- Una determinación más rápida y eficiente de las causas de los problemas que tienen los sistemas
- Corrección rápida e inteligente de problemas a través de la intervención remota
- Los técnicos de servicio llegan al emplazamiento ya bien informados y equipados de manera óptima
- Soporte rápido al usuario en caso de cuestiones relativas a aplicaciones

Lo primero es la seguridad de los datos
Tenemos el compromiso de mantener una colaboración a largo plazo basada en la confianza – y por esa razón la seguridad de los datos tiene para nosotros una importancia primordial. A la hora de instalar SRS, realizamos un análisis detallado de la situación, teniendo en cuenta la normativas internacional y nacional además de la infraestructura técnica antes de complementar nuestra oferta de servicio con conectividad remota. Nuestro equipo de servicio evalúa cuidadosamente las necesidades de cada cliente, de forma individual, respecto a la seguridad de la información y la seguridad del sistema.

He aquí una selección de los requisitos típicos de los clientes que Siemens cubre:
- **La privacidad de datos:** SRS ofrece y siempre tratará a la privacidad de los datos de sus clientes con el mayor respeto. Se aclaran todos los temas potenciales y medidas de seguridad antes de establecer cualquier conexión remota.
- **Acceso supervisado:** Nuestros clientes tienen la posibilidad de observar y terminar a su comodidad cualquier acceso al servicio remoto.
- **Pista de Auditoría Rastreable**: Los detalles de cada sesión individual se pueden recuperar fácilmente bajo petición del cliente o del legislador
- **Acceso selectivo** – administración individual de los derechos del usuario y sus accesos a datos: Los clientes pueden definir los derechos de acceso a sus sistemas y datos.

La seguridad de la información a través del concepto de seguridad multi-etapas.

Acceso controlado por el cliente
El requisito previo principal para cada actividad del servicio remoto es la autorización por parte del cliente. Nuestros clientes son los únicos que pueden definir en un contrato legalmente vinculante, qué técnico de servicio podrá acceder a qué partes de cuál sistema. Nuestros clientes también definen cuándo y en qué medido se le permite al técnico de servicio acceder a su sistema.

He aquí algunos de los modelos de acceso más comunes elegidos por nuestros clientes:

- **Acceso bajo solicitud:** Nuestro técnico de servicio sólo puede acceder al sistema de un cliente bajo solicitud individual. Por ejemplo, el técnico de servicio podría solicitar un acceso limitado en el tiempo para eliminar un problema específico. Este acceso no es permanente. Este arreglo puede ser acordado contractualmente e incluso se puede incluir en los valores establecidos del cortafuegos del cliente.

- **Acceso supervisado:** El cliente puede vigilar en tiempo real al técnico de servicio que está traba-jando en el sistema a través de la compartición remota de consola de sobremesa. El espectro de servicios donde se requiere esta opción y los medios técnicos para restringir el acceso a este nivel se acuerdan mu-tuamente.

- **Acceso pleno:** Un técnico de servicio expresamente autorizado tiene el permiso del cliente para conectarse al sistema en cualquier momento. Cada acceso al sistema se registra automáticamente para su revisión por el cliente. Los clientes habitual-mente eligen otorgar acceso pleno cuando su objetivos clave son el mantenimiento preventivo proactivo y la disponibilidad del sistema más alta posible.

- **Comunicaciones salientes:** El sistema del cliente puede enviar in-formación en tiempo real o en inter-valos acordados, al Centro de Servicios de Siemens a través de la plataforma SRS. Esto permite la recopilación de datos estadísticos para los servicios de optimización del siste-ma, de gestión proactiva de incidentes y de mantenimiento preventivo. Siemens, en colaboración con el cliente, se encarga de que solo se transmiten los tipos de datos acordados desde los sistemas acordados.

Selección de personal
Sólo permitimos trabajar en nuestra unidad SRS a aquellos empleados que hayan sido formados en la protección de datos y en la seguridad TI. Tenemos criterios estrictos de selección y nuestros técnicos de servicio tienen que participar obligatoriamente en procesos de formación y validación continua.

Autentificación y autorización
Cada vez que un técnico de servicio se registra en nuestra plataforma SRS, se verifica su ID de usuario y contraseña con los derechos de acceso correspondientes.

Los modelos de acceso definidos por el cliente se duplican y reflejan dentro de nuestra plataforma SRS y se convierten en niveles autorizados de acceso al sistema TI. Estos niveles de acceso se casan entonces con la iden-tidad verificada del técnico de servi-cio. El uso de este mecanismo asegura que los técnicos de servicio sólo puedan acceder a aquellas partes de los sistemas de cliente para las cuales estén expresamente autorizados.

Pista de auditorÍa rastreable
Siemens mantiene una disposición constante a informar a los clientes sobre cuál de los técnicos de servicio tuvieron acceso a cuáles datos, cuándo y qué actividades de comunicaciones fueron realizadas en cada sistema. Esta pista de auditoría se habilita mediante las medidas siguientes:

- Se registra cada uno de los accesos al sistema del cliente. Se aplican re-ferencias horarias de entrada y de salida además de la identidad del técnico.

- Los logs de registro se mantienen en ficheros durante por lo menos doce meses, y se puede ampliar el tiempo de almacenamiento bajo petición del cliente.

Las peticiones por parte del cliente de incluir información complementaria en la pista de auditoría se pueden tener en cuenta en la medida en que sean técnicamente posibles.

Acceso sólo a socios verificados
Algunos servicios podrían precisar la involucración de socios externos de servicio técnico e ingeniería.

Para asegurar que se mantenga en dichos casos el mismo nivel fiable de seguridad, nuestra plataforma SRS ofrece un mecanismo de acceso por socios. Sólo después de completar con éxito un proceso de autentificación muy exhaustivo y rigurosamente aplicado pueden acceder los socios verificados a áreas específicamente definidas de un sistema de cliente a través de la plataforma SRS.
Todos los servicios de socio verificado se registran exactamente con la misma precisión que los accesos al sistema realizados por nuestros técnicos de servicio.

Protección de la transmisión de datos
Nuestra plataforma SRS utiliza métodos de encriptación del más avanzado estado del arte para proteger los datos del cliente frente a accesos no autorizados durante la transmisión. Se pone un énfasis específico en la encriptación integrada como requisito previo para cualquier comunicación a través de Internet.

En el caso de solicitud por parte del cliente de una mayor seguridad como respuesta a amenazas específicas, nuestra plataforma SRS también puede proporcionar soluciones de encriptación router a router basada en hardware para la transferencia de datos.

Arquitectura de red segura

La plataforma SRS central se encuentra dentro de la infraestructura de red propia de Siemens y está protegida frente a accesos no autorizados desde el exterior.

Dentro de una zona desmilitarizada (DMZ), un servidor de acceso SRS actúa como un control de acceso Seguro entre Internet y la red de Siemens, donde se almacenan los datos de Siemens. Establece una conexión segura entre el sistema del cliente y el sistema del técnico de servicio.

Una DMZ con tecnología de servidor Proxy es una arquitectura de red probada que asegura que sólo se permite a los datos solicitados previamente por un proceso de servicio remoto autentificado por Siemens, pasar a la red de Siemens. Esto previene el acceso no autorizado o fraudulento a los datos del cliente a través de Internet.

Gestión de datos

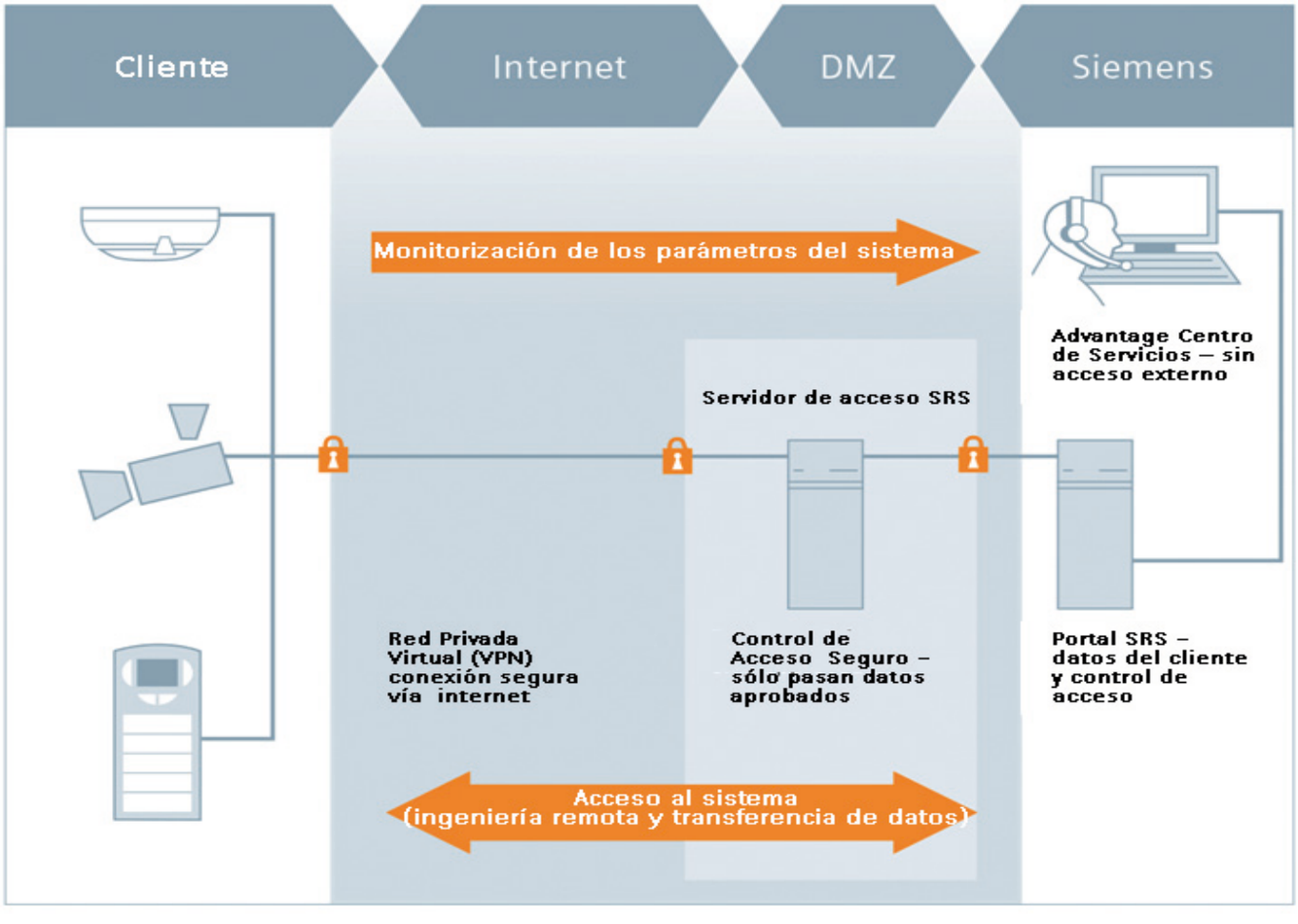
Clasificamos como altamente confidenciales los datos del cliente y otor-gamos acceso sólo a los que necesitan conocerlos. La imposición de este principio es apoyada por mecanismos de control de acceso basado en políticas que se mapean dentro de un paisaje de infraestructuras y herramientas que fueron especialmente desarrolladas para este fin.

Las medidas implantadas para la gestión de datos dependen de los requisitos individuales del cliente en cuanto a la protección de datos, el tipo de datos y las normativas de la legislación pertinente. Respecto a los temas tales como soluciones individuales para la retención de datos, respaldos, los derechos de propiedad y eliminación, podemos ofrecer un completo asesoramiento.

Disponibilidad de la plataforma

La disponibilidad de nuestra plata-forma SRS está asegurada gracias a tres centros de datos totalmente redundantes ubicados en Alemania, Singapur y los Estados Unidos. La capacidad de cada centro se planifica de forma que la plataforma SRS no se verá afectada en absoluto si surge alguna perturbación a menos que dos centros de datos se salgan repentinamente de línea,.

La integración de planes suplemen-tarios de recuperación ante desastres (DR) y de gestión de continuidad del negocio (BCM) aseguran un tiempo de incomunicación el más bajo posible incluso si, cosa muy improbable, surgen catástrofes simultáneas que afecten a nuestros centros de datos.



Auditoría y certificación.

ISO 27001

Siemens fue una de las primeras organizaciones en todo el mundo en tener un sistema de gestión de la seguridad de la información (ISMS) para servicio remoto aceptado interna-cionalmente, certificado por la norma ISO/IEC 27001:2005. Nuestra plataforma SRS retiene la certificación continua por TÜV Süd en Alemania y se lista en el Registro Internacional de Certificados ISMS encontrado en www.iso27001certificates.com.

Auditoría CERT de Siemens

El Equipo de Respuesta a Emergencias en Ordenadores (CERT) de Siemens es un socio interno, independiente y fiable que desarrolla medidas de seguridad preventiva y valora la seguridad de la información en la infraestructura TI. Nuestra plataforma SRS se audita periódicamente para asegurar una protección válida y continuas mejoras.

Hardware de red proporcionado por Siemens

Siempre que el uso de hardware proporcionado por Siemens para la encriptación router a router resulte adecuado, tu puedes contar con tecnología estándar de la industria para la protección de tus datos. Sólo se emplean routers estándares de la industria con capacidades certificadas de IPSec, VPN y HTTPS Proxy

.

Contactos e información

Si desea más información sobre nuestra plataforma SRS y portfolio de servicios remotos, póngase en contacto con su representante local de ventas de Siemens.

Será un placer ayudarle a configurar sus equipos para establecer una conexión SRS segura.