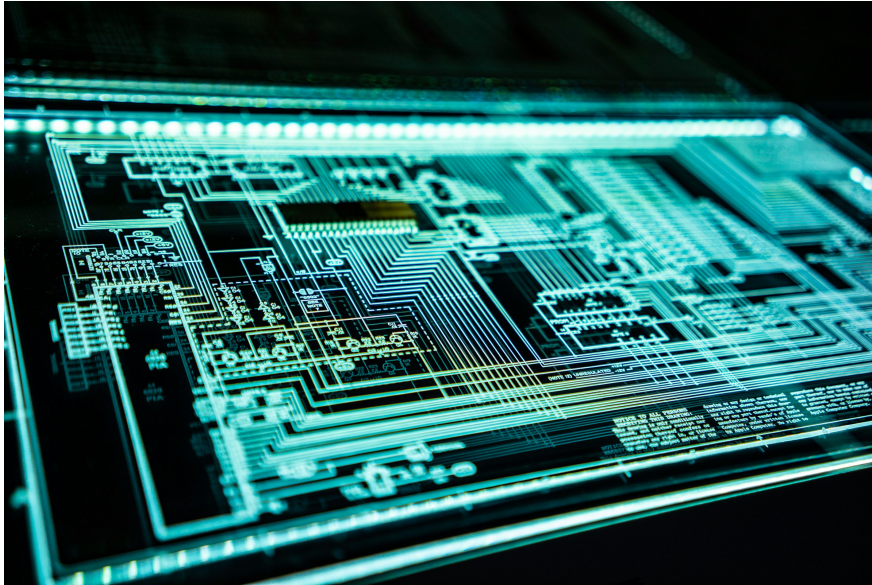




El BSI de Alemania recomienda eliminar el acceso directo desde internet a los sistemas de control de plantas...

- La Oficina Federal de Seguridad de la Información de Alemania "recomienda encarecidamente proteger los sistemas de control conectados en red": ha publicado una recomendación sobre ciberseguridad dirigida a los operadores de instalaciones pequeñas y muy pequeñas, incluidas plantas hidroeléctricas, eólicas, de...



<https://www.pv-magazine.es/2026/10/16/el-bsi-de-alemania-recomienda-eliminar-el-acceso-directo-desde-inte...>

Pilar Sánchez Molina

Viernes, 16 octubre 2026

La Oficina Federal de Seguridad de la Información de Alemania, BSI por sus siglas en alemán, ha publicado una recomendación de ciberseguridad para proteger sistemas de control industrial accesibles desde internet. En concreto, "recomienda encarecidamente proteger los sistemas de control conectados en red". El documento se dirige especialmente a operadores de instalaciones pequeñas y muy pequeñas, incluidas plantas hidroeléctricas, eólicas, de valorización energética de residuos y plantas fotovoltaicas de cualquier tamaño.

La principal medida recomendada es impedir el acceso directo desde internet a los sistemas de control. En una planta solar, estos sistemas pueden incluir controladores industriales, equipos de comunicaciones, pasarelas de monitorización, inversores, sistemas SCADA y plataformas de supervisión remota.

La conexión directa de estos activos a internet amplía la superficie de exposición a ataques. Un sistema identificado desde la red pública puede ser objeto de intentos de acceso no autorizado, explotación de vulnerabilidades conocidas o manipulación de parámetros operativos. El riesgo no se limita a la indisponibilidad de datos de monitorización: un incidente en tecnología operativa, u OT, puede afectar al control de la instalación y a su disponibilidad.

El BSI recomienda sustituir la exposición directa por accesos remotos protegidos mediante redes privadas virtuales, VPN, y autenticación multifactor. La VPN crea un canal cifrado entre el usuario

autorizado y la red de la instalación, mientras que la autenticación multifactor añade una segunda prueba de identidad además de la contraseña. Estas medidas no eliminan por sí solas el riesgo, pero reducen la probabilidad de accesos indebidos por credenciales robadas o contraseñas débiles.

La recomendación incluye mantener actualizados los equipos y aplicar con rapidez las actualizaciones de seguridad y las correcciones de errores. Esta medida afecta tanto a los sistemas de supervisión como a los dispositivos de campo conectados, incluidos routers, cortafuegos, controladores, inversores y pasarelas de comunicación. La falta de actualizaciones puede mantener expuestas vulnerabilidades que ya cuentan con medidas de corrección disponibles.

El BSI también pide comprobar de forma periódica si existen dispositivos o instalaciones visibles desde internet. Esta revisión requiere inventariar los activos conectados, identificar sus interfaces de comunicación y verificar que no haya servicios remotos expuestos de forma innecesaria. Cuando se detecte una exposición, el operador deberá aplicar medidas de mitigación específicas.

Para las plantas fotovoltaicas, la recomendación refuerza la necesidad de separar la red corporativa de la red de operación, limitar los accesos remotos a usuarios y proveedores autorizados y establecer procedimientos periódicos de actualización y revisión. El organismo alemán plantea que estas actuaciones se incorporen a la operación habitual de los activos para elevar el nivel de seguridad de los sistemas de control conectados.