# “En la industria del petróleo y del gas **los sistemas SIS merecen el mayor foco de atención”**

Por ***Sebastián Hernández*** (Especialista en Sistemas de Control Distribuido y Sistemas Instrumentados de Seguridad, Emerson Process Management)

**Se le consultó al departamento de Ciberseguridad de la empresa de soluciones y procesos si se registraron cambios a partir de la pandemia y consiguiente cuarentena. Estas fueron las respuestas.**

**¿Cambió algo en ciberseguridad a partir de la pandemia?**

Indudablemente, la pandemia trajo varias situaciones novedosas a las cuales las empresas debieron adaptarse. Una gran cantidad de gente se vio en la necesidad de acceder remotamente a sus sistemas (ya sean los de gestión o los de monitoreo y control) para continuar con sus actividades y no todas las empresas estaban preparadas para responder a esa necesidad. Eso generó la exposición de los sistemas informáticos a muchas amenazas, incrementando la atención de los grupos de Tecnología Informática para mejorar las instalaciones detectando las vulnerabilidades.

**¿Cuáles son las principales amenazas que se ven?**

Una de las principales amenazas que se observaron estos meses es que muchas compañías se encontraron con la situación de que sus empleados no contaban con computadoras o laptops provistos por las empresas, entonces comenzaron a utilizar equipos hogareños. Esos equipos, por lo general no cuentan con los paquetes de software de seguridad necesarios para proteger la información ni las actualizaciones de antivirus necesarias.

### ¿En ciberseguridad, la Argentina es muy diferente de la región o del resto del mundo?

En materia de ciberseguridad en la Argentina se tiene, afortunadamente, profesionales con mucho conocimiento de la materia y una gran capacidad para realizar diagnóstico y detectar los problemas de ciberseguridad en una instalación o hasta en una organización entera.

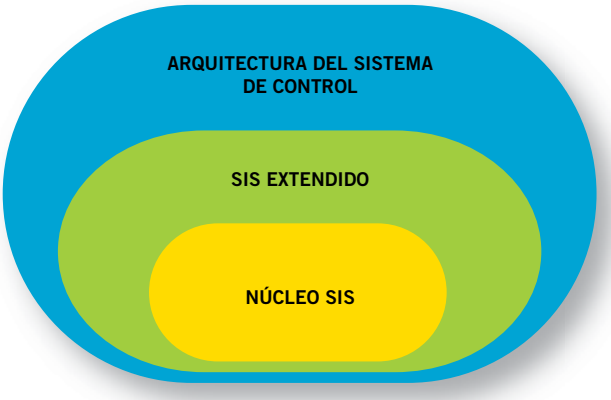
En la industria local se sufren pérdidas de información y de producción debido a problemas de ciberseguridad, aunque la mayoría de ellos no se corresponden a ataques deliberados. Son los descuidos, la falta de inversión en protecciones y, a veces, el poco entendimiento de cómo realizar mantenimiento de los sistemas a lo largo de su ciclo de vida. Frecuentemente son esos temas los que merecen mayor atención.

### ¿Qué estrategia de seguridad sugieren?

Con el aumento de los ataques cibernéticos, una sola capa de protección para los activos críticos de seguridad no es suficiente. Los administradores de redes están empleando muchas capas de seguridad (antivirus, gestión de usuarios, autenticación por múltiples factores, prevención y detección de intrusiones, *whitelisting, firewalls* y más) para garantizar que usuarios no autorizados se enfrenten a una barrera de entrada insuperable. A este modelo se le llama estrategia de defensa profunda *(defense-in-depth)* y su objetivo es aumentar los mecanismos de protección de control de acceso, lo cual se puede lograr agregando capas de protección que se complementan entre sí.

Especialmente en la industria del petróleo y del gas los sistemas instrumentados de seguridad (SIS) son los que merecen el mayor foco de atención.

La Asociación de Usuarios de la Tecnología de Automatización en Industrias de Procesos, NAMUR por sus siglas en inglés, ofrece un set de lineamientos similares a los de ISA 62443, con funciones SIS agrupadas en tres zonas: Núcleo SIS, SIS Extendido y Arquitectura del sistema de control.




Uno de los métodos más comunes para proteger un SIS es separar completamente el sistema, lo que permite que haya espacio físico o "AIR GAP" entre las funciones del Núcleo SIS y del BPCS. A primera vista, los beneficios de este enfoque parecen obvios. Si el SIS está completamente separado de otros sistemas, estará fortalecido contra intrusiones en forma inherente.

Sin embargo, los sistemas separados no son inmunes a los ataques cibernéticos. Los usuarios eventualmente necesitarán acceso externo al sistema para extraer registros para la secuencia de análisis de eventos, bypass, anulaciones, registros de pruebas de verificación o simplemente para realizar cambios en las configuraciones y aplicar actualizaciones de seguridad. Las unidades de USB, que son los medios habituales para implementar las actualizaciones, no son fáciles de proteger.

En el caso de la industria petrolera, específicamente en las operaciones de *upstream*, existen muchas comunicaciones que van en el campo a cielo abierto, utilizando distintos medios de comunicación a través de RTUs, sistemas SCADA, etc. Desde hace algunos años existe un uso creciente de protocolos de comunicación que en su diseño incluyen esquemas de seguridad. Por ejemplo si hablamos de protocolos abiertos, el protocolo DNP3 está reemplazando en gran medida al protocolo Modbus para este tipo de redes de comunicación, como una buena opción frente a protocolos propietarios. ■