¿Quién es el dueño de la ciberseguridad industrial?

Conflicto y acciones de la ciberseguridad en la industria

Enrique Larrieu Let
elarrieulet@gmail.com

Enrique Larrieu-Let es ingeniero, CISM, profesional de seguridad y tecnologías de sistemas de información. Miembro de la Asociación de Auditoría y Control de Sistemas de Información. ADACSI, IAIA, Universidad del Salvador.

En materia de ciberseguridad industrial, no creo que nadie se sienta con derecho a tener toda la verdad y todas las respuestas a las posibles amenazas y ataques, y también creo que todos lo saben. Pero entonces, ¿quién debe ocuparse del tema y hacerse responsable?

Las diferentes prioridades de IT y OT son la causa de los conflictos entre ambos grupos.

La situación

Observamos un cambio significativo en estas infraestructuras que evolucionaron de sistemas monopólicos y monolíticos aislados a configuraciones de mercado abierto integradas al resto del mundo. Este cambio de paradigma permite proporcionar al usuario final servicios más efectivos, eficientes, centrados en el usuario y fáciles de usar, con una reducción significativa de los costos. Sin embargo, esto las expone a una gran cantidad de amenazas peligrosas potenciales.

Esto se debe a que el escenario socio-técnico actual comienza a caracterizarse por un gran aumento en las interacciones y especialmente de las dependencias (recíprocas) entre las diferentes infraestructuras.

Este fenómeno contribuye severamente a aumentar la complejidad de todo el escenario que, si bien es más robusto a los eventos de bajo impacto y de alta frecuencia, aparece cada vez más propenso a fallas sistémicas y catastróficas como lo demuestra la estadística de incidentes en el mundo.

Prioridades de seguridad

Las diferentes prioridades de IT y OT (tecnologías de la información y tecnologías operacionales) son la causa de los conflictos entre ambos grupos, y eso se explica porque tienen objetivos diferentes, como lo muestra la figura 1, ya que IT tiene a las TIC (tecnologías de la información y la comunicación) y OT tiene a los ICS (soluciones de información y comunicación).

La principal prioridad de TI es proteger los datos. Sin embargo, la prioridad de OT es proteger la disponibilidad e integridad del proceso con énfasis en la seguridad de las personas y la planta, la confidencialidad queda en el último lugar.

Cada grupo tiene una lente sesgada cuando considera los riesgos y consecuencias en ciberseguridad.

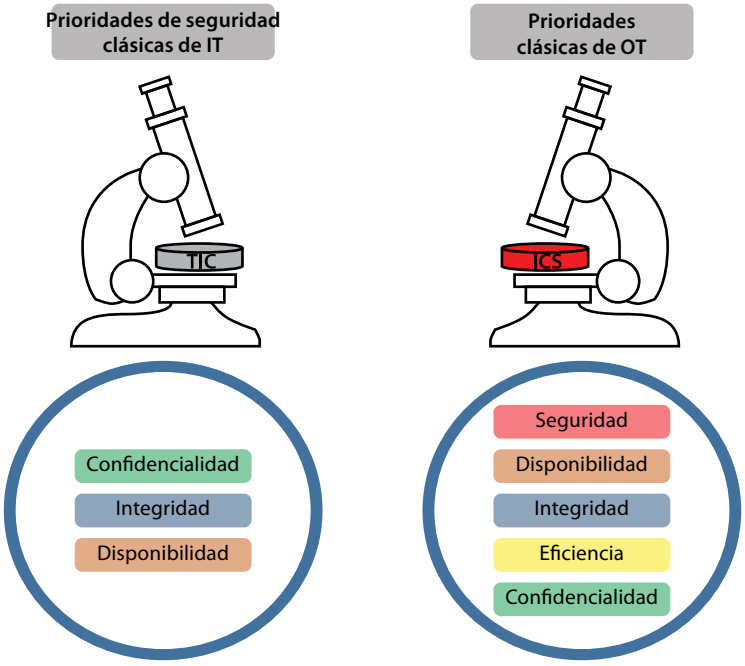

Figura 1. Propiedades clásicas de IT y OT

El conflicto

Ambos mundos, el de IT y el de OT, vivían felices y contentos cuando cada uno se ocupaba de lo suyo sin interacciones ni físicas ni virtuales.

Pero el entorno, de la mano de la tecnología, creó demandas sociales y comerciales que los obliga a vincularse y, como en toda convivencia, surgen los conflictos. En este caso, totalmente justificados dado que, si bien la protección de la información es importante, las pérdidas de producción que se traducen inmediatamente en pérdidas comerciales también lo son.

Pero el conflicto es aún peor porque, no solo es por diferencia de intereses, sino que además existe una doble desconfianza entre ambos, tanto en lo operativo, como en los riegos.

En cuanto a lo operativo, por lo general, los equipos de OT dudan en aceptar los cambios de IT en el entorno operativo por resistencia a detener la producción de manera planificada o temor de que se produzca una interrupción prolongada causada por un problema con la implementación. Y en cuanto a los riesgos, las amenazas cibernéticas provenientes por conectarse a IT también pueden interrumpir la producción, causar daños, afectar la visibilidad y el control o poner en peligro la seguridad de la infraestructura, las personas y el medioambiente, además, por supuesto, de afectar la rentabilidad del negocio. Y por otra parte las vulnerabilidades de los ICS hacen temer a IT que los ciberdelincuentes penetren por allí para robar secretos comerciales.

Todo esto es cierto y posible y ya lo sabemos. Veamos ahora algunas acciones para comenzar a mediar entre ambos y minimizar los impactos del conflicto.

Acciones

Desafortunadamente, los consultores que realizan evaluaciones de riesgos en entornos de operaciones de ICS dicen que muchas organizaciones deben experimentar un ciberincidente de alto impacto antes de estar dispuestas a tomar medidas significativas.

Entonces, ¿cuáles son las acciones posibles que una organización industrial podría tomar para facilitar la convivencia de IT y OT y minimizar el impacto de los conflictos y la desconfianza y al mismo tiempo aumentar la seguridad de los ICS?

Si bien la protección de la información es importante, las pérdidas de producción que se traducen inmediatamente en pérdidas comerciales también lo son.

Establecer una alineación estratégica en los niveles más altos

La mayoría de las industrias aún poseen dos áreas fuertemente disociadas de operaciones y de tecnología de la información. Tienen diferentes personas, objetivos, directivas y proyectos.

Para mejorar esto, se recomienda desarrollar (si no la tiene aún) una estrategia de ciberseguridad para toda la organización, y que se encuentre alineada con la estrategia global del negocio para que sirva y agregue valor a las necesidades de este.

Cumplido este requisito indispensable, se debe comenzar reorganizando los departamentos de IT y OT, para que estén estratégicamente alineados y unificados con la estrategia global de ciberseguridad. Se sugiere que, como mínimo, el director de información (CIO), el director de seguridad de la información (CISO) y el director de operaciones (COO) tenga objetivos y metas parcialmente comunes y alineadas, lo que los obligaría a trabajar de manera cooperativa.

El CIO y el CISO también deben aceptar la responsabilidad total de la ciberseguridad del ICS y de cualquier incidente de seguridad, incidentes de integridad o fallas o daños al equipamiento e instalaciones causados directa o indirectamente por incidentes cibernéticos.

Coordinar un equipo de trabajo conjunto

El NIST (Instituto Nacional de Normalización y Tecnología, dependiente del Departamento de Comercio de Estados Unidos), en su documento SP800-82r2, recomienda crear un equipo de trabajo conjunto, como un equipo de ciberseguridad multifuncional y multidisciplinario, para compartir su variado conocimiento y experiencia, con la finalidad de evaluar y mitigar el riesgo para los ICS.

En el documento, además, se sugiere designar específicamente algunos cargos que deberían ser parte de este equipo de trabajo de ciberseguridad: un miembro del personal de TI, un ingeniero de control, un operador del sistema de control, un experto en seguridad de redes y sistemas y un miembro del departamento de seguridad física.

Se debe comenzar reorganizando los departamentos de IT y OT, para que estén estratégicamente alineados y unificados con la estrategia global de ciberseguridad.

Proyectos piloto

Una de las primeras cosas que puede hacer el grupo de trabajo conjunto de ciberseguridad es identificar proyectos piloto simples para trabajar vinculados. Una sugerencia podría ser crear de mutuo acuerdo una lista de los activos de ICS más críticos que deben estar absolutamente protegidos, clasificarlos en orden de prioridad y evaluar sus riesgos e impactos, para luego comenzar a implementar acciones de monitoreo y control en ciberseguridad.

Estos proyectos piloto brindarán valor al negocio, ayudando a la organización a capacitarse y desarrollar progresivamente una suite específica de habilidades compartidas de IT/OT. Esto también ayudará a determinar cómo minimizar los impactos del conflicto al estar motivados a decidir de manera consensuada los pasos hacia la mejora de la ciberseguridad de los ICS.

Gobierno de las tecnologías

Una cosa es la gestión y otra, el gobierno de las tecnologías en general y de la ciberseguridad en particular.

Mientras que la gestión debe recaer en cada área de trabajo de IT y OT, el gobierno debe recaer en el equipo conjunto de ciberseguridad, que debería tener autoridad para ejecutar proyectos, armonizar sistemas y procesos y promover el desarrollo de las habilidades interdisciplinarias necesarias para proteger los ICS y satisfacer las necesidades del negocio a la vez.

Conclusión

La mitigación exitosa de los conflictos inherentes a la convergencia de IT y OT, y la posterior mejora de la seguridad de ICS, no ocurre de la noche a la mañana. Este es un desafío complejo para cualquier organización. Los gerentes deben aprender a compartir objetivos, evaluar conjuntamente los riesgos y hacer frente a los impactos en el negocio juntos. Para esto, se requiere de mucho trabajo previo de concientización y de capacitación para cambiar conductas que conduzcan a productos, procesos, políticas y personas de seguridad de ICS apropiados. ■