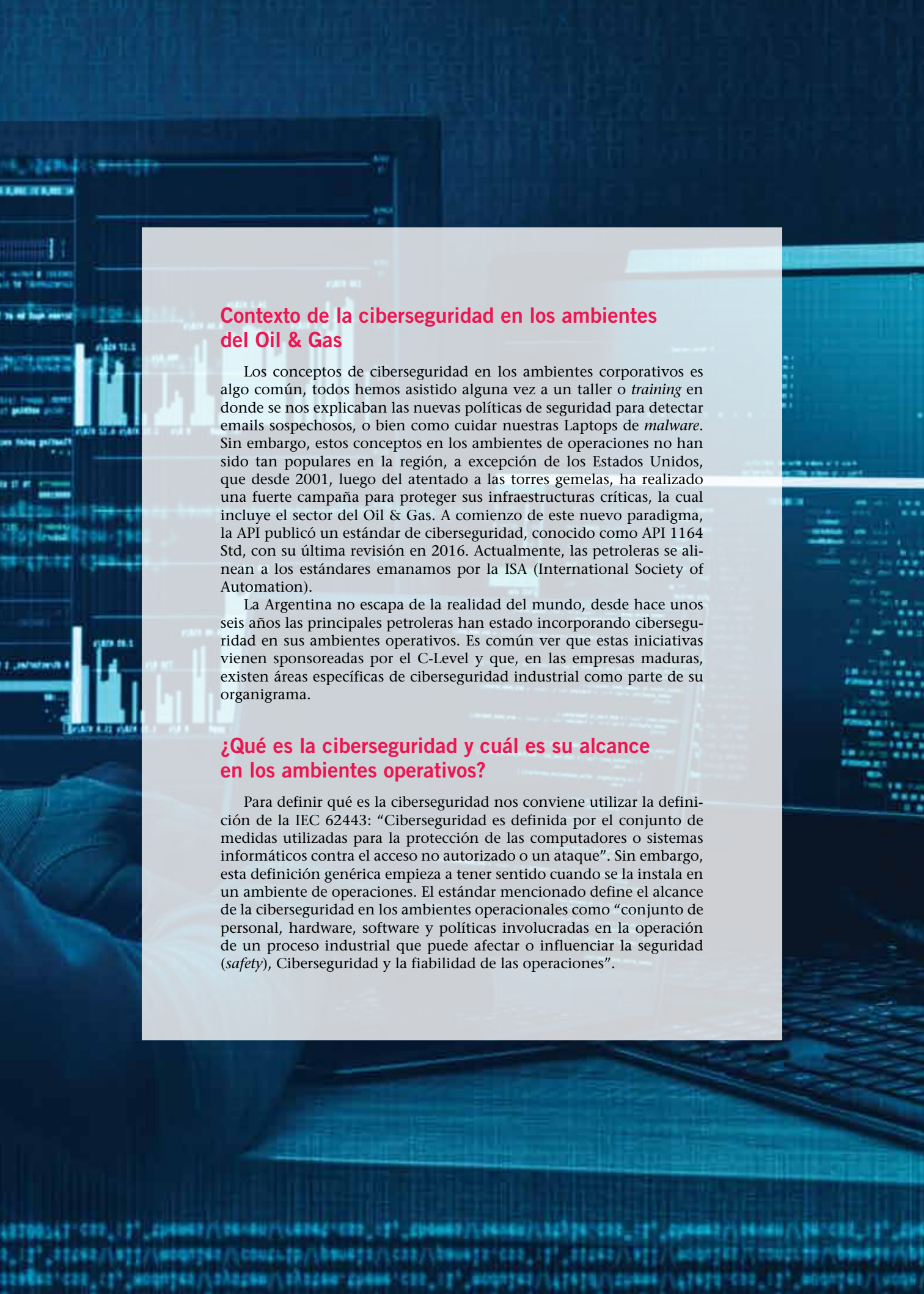
CIBERSEGURIDAD INDUSTRIAL

Impacto “real” de la ciberseguridad en los ambientes del Oil & Gas y su situación en la región

Pablo Almada (KPMG)

En este trabajo se analizan casos reales del impacto y el nivel de exposición a los ciber-ataques que tienen las empresas del sector hidrocarburífero desde una perspectiva “real” de la operación del día a día de un yacimiento.



Contexto de la ciberseguridad en los ambientes del Oil & Gas

Los conceptos de ciberseguridad en los ambientes corporativos es algo común, todos hemos asistido alguna vez a un taller o *training* en donde se nos explicaban las nuevas políticas de seguridad para detectar emails sospechosos, o bien como cuidar nuestras Laptops de *malware*. Sin embargo, estos conceptos en los ambientes de operaciones no han sido tan populares en la región, a excepción de los Estados Unidos, que desde 2001, luego del atentado a las torres gemelas, ha realizado una fuerte campaña para proteger sus infraestructuras críticas, la cual incluye el sector del Oil & Gas. A comienzo de este nuevo paradigma, la API publicó un estándar de ciberseguridad, conocido como API 1164 Std, con su última revisión en 2016. Actualmente, las petroleras se alinean a los estándares emanamos por la ISA (International Society of Automation).

La Argentina no escapa de la realidad del mundo, desde hace unos seis años las principales petroleras han estado incorporando ciberseguridad en sus ambientes operativos. Es común ver que estas iniciativas vienen sponsoreadas por el C-Level y que, en las empresas maduras, existen áreas específicas de ciberseguridad industrial como parte de su organigrama.

¿Qué es la ciberseguridad y cuál es su alcance en los ambientes operativos?

Para definir qué es la ciberseguridad nos conviene utilizar la definición de la IEC 62443: “Ciberseguridad es definida por el conjunto de medidas utilizadas para la protección de las computadores o sistemas informáticos contra el acceso no autorizado o un ataque”. Sin embargo, esta definición genérica empieza a tener sentido cuando se la instala en un ambiente de operaciones. El estándar mencionado define el alcance de la ciberseguridad en los ambientes operacionales como “conjunto de personal, hardware, software y políticas involucradas en la operación de un proceso industrial que puede afectar o influenciar la seguridad (*safety*), Ciberseguridad y la fiabilidad de las operaciones”.

El impacto de la ciberseguridad en la industria del Oil & Gas

Para poder analizar la importancia y el impacto de la ciberseguridad en los ambientes industriales solo basta con analizar los últimos incidentes que ocurrieron en la industria. Entre los más famosos se encuentran los dos ocurridos en Saudi Aramco, el primero de ellos bloqueó el uso de 30.000 computadoras y, el segundo, más específico y complejo, logró tomar el control de su SIS (Sistema Instrumentado de Seguridad) Schneider Triconex con el objetivo de perpetrar un sabotaje en una de sus plantas.

En la región tampoco estamos excepto de este tipo de ciberataques, por supuesto no tan avanzados como los de Saudi Aramco, ya que hasta el momento no somos blanco de conflictos políticos o bélicos. Sin embargo, ha sufrido múltiples ataques orientados a las empresas del sector, basta con recordar el ataque que sufrió PEMEX en noviembre del 2019, en donde sus sistemas centrales fueron víctimas Ransomware. Obviamente que en este tipo de incidentes suele filtrarse muy poca información, mínimamente lo que deben saber sus accionistas y la SEC.

En los últimos meses, otras empresas de la región han sufrido ataques, por ejemplo, ENEL, EDESUR, Telecom, HONDA y Prosegur, entre otras. ¿Qué relación tienen las empresas antes nombradas con las empresas del rubro? La respuesta es la interconexión de sus servicios que expone nuestras facilities. Analicemos el siguiente caso.

Una planta de tratamiento de gas utiliza generadores eléctricos contratados a una famosa empresa del rubro, claramente estos generadores son monitoreados por ambas empresas, la propietaria de la planta y el dueño de los generadores. Luego, posee un servicio de vigilancia para entrar al yacimiento y para el control de los vehículos en circulación. La empresa operadora debe darle servicio de conectividad a la empresa de vigilancia para el control de sus empleados. Asimismo, los compresores de la planta tienen un monitoreo remoto de mantenimiento por parte de la garantía del vendedor, otra vez la compañía operadora se encuentra dando conectividad a este servicio. Además de la conectividad con el campo, en donde hay un sistema de control para ver el estado de los Pads y cámaras. En este caso, se esta monitoreando el estado de válvulas, el estado de sus sistemas hidráulicos y el estado de los desands, entre otros. Todo este monitoreo del yacimiento se hace a través de medios de comunicación propios y de terceros por medio de la tecnología 4G de una famosa compañía de telecomunicaciones. Adicionalmente, se tiene la conexión con el punto de entrega de gas a la transportista, donde están el cromatógrafo, el sensor ultrasónico, un control Flow y los equipos de medición del transportista interconectado con los equipos de la operadora. Por último, está el proveedor de servicios de una famosa integradora que trabaja en planta y por sus tareas tiene conectada su laptop a nuestros sistemas continuamente, la misma laptop que usa para navegar por internet, ver mails personales y trabajar en otras plantas de otras operadoras.

Como se ha detallado anteriormente de forma simplificada, existe múltiples puntos de interconexión entre empresas, redes y recursos que exponen nuestra *facility* a

riesgos de ciberseguridad. Solo falta que alguno de todos los participantes de este modelo tenga un problema de ciberseguridad para que la operadora se vea impactada.

¿Qué impacto "real" tendríamos?

Siguiendo con el ejemplo anterior, imaginemos que una de estas empresas se ve comprometida por un usuario que hizo clic en un lugar indebido, o bien abrió un archivo que recibió por mail e infectó su laptop de trabajo. Esto provocó que se propague un malware por la red de su empresa y, a su vez, que esta propagación tome el camino de una interconexión a nuestra planta, por ejemplo, por donde se encontraban monitoreando a través de un enlace los equipos de generación eléctrica. La operadora tenía una conexión modbus TCP para la toma de datos de los generadores, lo que hizo que el malware aproveche esta conexión y llegue a las redes de control de la planta. Bajo este escenario, ¿qué podría pasar en la planta? Claramente no explotaría, las plantas deberían ser seguras por defecto, por algo se hizo un Hazop, pero sí podría dejar de operar. Una vez que se materializa este evento en la planta, basándonos en una arquitectura modelo de Siemens, el malware se propagará por las estaciones de operación, estaciones de ingeniería y servidores provocando una pérdida de visualización de la planta y del yacimiento.

Consecuentemente, por seguridad deberíamos ir a una parada de planta. Bajo esta condición vemos que todos nuestros equipos informáticos de control y operación se encuentran bloqueados, el personal de instrumentación y control no sabe que es lo que pasó, cuando empiezan a sospechar que esto pudo haber sido producido por un malware, luego de unas seis horas con la planta parada, se comunican con el área de IT para que los ayuden. El problema es que IT no tiene ni la menor idea de cómo es la arquitectura de la planta, que podría haberse visto afectado, y se preguntan entre todos: ¿este evento afectó a los S7-1200 de la planta?, ¿por dónde entró?, ¿está el perpetuador del evento "virtualmente" dentro de la planta?, ¿cómo nos recuperamos?, ¿sabemos como es el plan de recuperación?, ¿tenemos backups? Si no sabemos de donde vino la infección, ¿cómo nos aislamos para que esto no pase nuevamente?, ¿podemos cortas las comunicaciones con el resto de nuestras empresas de servicio sin que se vean afectados los contratos y recibamos multas o perdamos las garantías?, ¿dónde son los puntos de interconexión?, cuando hicimos los backups ¿tuvimos en cuenta los últimos cambios?, ¿Tenemos los proyectos del portal tia últimos en un backups?, ya vamos por 36 h con la planta parada… Esperen, ¿los backups están en el servidor infectado?, entonces perdimos todo, debemos empezar a levantar y programar la planta desde cero.

El escenario antes descripto, en mi experiencia, podría pasar en cualquier planta de las operadoras de la Argentina. Es más, he tenido la oportunidad de toparme con casos en los cuales en paradas de mantenimiento se han infectado sistemas y se debió programar todo desde cero y, en consecuencia, se produjeron pérdidas económicas.

El nivel de exposición de las facilities cada día es mayor, solo basta con mirar el nivel de automatización que tenemos en un Pad no convencional con respecto al pozo del Golfo San Jorge para darse cuenta que aún no se tienen los niveles de automatización como los que se ven en los smart wells de medio oriente.

Ciberseguridad industrial en las empresas de oil & gas de la región

La empresa más importante de la Argentina ya posee un equipo específico para atender los requerimientos del Negocio en lo que respecta a la ciberseguridad. No debería iniciarse, por ejemplo, una implementación sin su análisis desde la perspectiva de la ciberseguridad. Otras grandes petroleras de la región están tomando actividades de ciberseguridad desde sus áreas de Ciberseguridad IT tradicionales con el apoyo de consultores especializados en la materia.

Claramente hoy ciberseguridad es una preocupación en la mesa de los directorios, por eso se ven aprobaciones de partidas presupuestarias cada día más incrementadas luego de un ataque que se hace público.

Por otro lado, se han visto caer negocios como consecuencia de que los vendedores no podían cumplir con las demandas de ciberseguridad en sus productos o servicios que requerían las empresas petroleras.

Los equipos de ciberseguridad industrial tienden a ser formados por personas que vienen de las áreas del negocio con otras personas que vienen del área de Ciberseguridad IT, logrando en consenso una mirada amplia de los riesgos del campo.

Es importante analizar como se debe formar un gobierno de ciberseguridad para que sea exitoso. El apoyo del C-level es clave para dar los primeros pasos en la materia. Luego, la institucionalización viene dada a través de un marco normativo colegiado con los distintos referentes del negocio para establecer de forma realista las bases de ciberseguridad industrial.

También, es fundamental conocer el estado de situación de la organización, qué nivel de exposición tiene y cuál es el riesgo al que se encuentra expuesta, entre otros aspectos. Adicionalmente, las petroleras que cotizan en la bolsa de los Estados Unidos bajo el control de la SEC, deben reportar obligatoriamente el estado de ciberseguridad de sus instalaciones industriales. Y, si son víctimas de un ciberataque, deben reportarlo inmediatamente.

Una vez que conocemos el punto de partida, debemos diseñar un plan director que nos guíe para elevar nuestro nivel de madurez, pero las preguntas que se reciben del directorio son ¿en dónde deberíamos estar?, ¿cuánto sale?, ¿qué riesgos mitigamos? Preguntas que se pueden responder desde la comparativa regional del resto de las compañías y del resultado de nuestra evaluación de ciberseguridad.

En la actualidad las empresas del sector ejecutan múltiples planes de ciberseguridad. Por ejemplo, podemos nombrar planes, como rediseño en la integración de sus redes de control, políticas de ciberseguridad, planes de awareness para sus operadores e instrumentistas, sistemas de monitoreo de ciberseguridad, esquema de actualizaciones de sus sistemas, implementaciones de *antimalware*, esquemas de gestión de accesos lógicos, accesos remotos potenciados por la cuarentena y SOC (*security operation centers)*, entre otros.

Finalmente observamos que los gobiernos de la región también entienden el problema que podría generar un ciberataque a una infraestructura de producción, no se trata solo de la imagen, sino más bien, desde la perspectiva de la operación del país. ¿Cómo vamos a responder si la facility más importante de la Argentina en lo que es refino deja de operar por un tiempo prolongado?, ¿cómo afecta esto a la producción del país?

Chile, Brasil y Colombia, entre otros, están generando marcos normativos de ciberseguridad para sus infraestructuras críticas. La Argentina también está en ese camino, lo que implica que pronto todas las petroleras deberán regirse por un marco gubernamental de ciberseguridad.