Un enfoque integrado para combatir el ciberriesgo

Cómo proteger las operaciones industriales en el sector del petróleo y el gas

Centro para Soluciones de Energía de Deloitte

Introducción

Las infraestructuras críticas dependen de sistemas de control industrial (ICS, en sus siglas en inglés) para que las operaciones se desarrollen de manera segura y fiable. Los ingenieros han diseñado e implantado con éxito dichos sistemas pensando en la seguridad y la fiabilidad de los sistemas, pero no siempre han tenido en cuenta la protección frente a las amenazas externas. ¿Por qué? Porque, inicialmente, no había necesidad de ello. Antes, los sistemas operativos aislados, diseñados para un fin específico, eran la norma. Dado que estos sistemas no estaban integrados en los sistemas empresariales, o ni siquiera estaban integrados entre ellos, el riesgo de que se produjera un fallo en cascada a gran escala debido a un ataque, tanto cibernético como de otro tipo, era muy poco probable.

Veinte años después, la conectividad ubicua del Internet de las Cosas (IoT) ha trastocado completamente los supuestos más básicos sobre seguridad operativa. Hoy día, todos los tipos de instalaciones industriales, incluidos los yacimientos petrolíferos, los oleoductos o gasoductos y las refinerías, son vulnerables a los ciberataques. Independientemente de su ubicación, actualmente los sistemas operativos pueden verse comprometidos por riesgos externos o internos, causando fallos de seguridad o producción y aumentando el riesgo comercial. Aunque los ICS normalmente están diseñados a prueba de fallos, la cada vez mayor sofisticación de los ciberdelincuentes aumenta el riesgo de que se produzcan accidentes catastróficos, a lo que hay que sumar la magnitud de los efectos en términos de costes, protección, reputación y pérdidas comerciales o económicas.

Al igual que otras industrias, el sector de los hidrocarburos ha estado trabajando para mejorar la ciberseguridad, que se ha convertido en una cuestión prioritaria para los altos directivos y consejos de administración.

Aunque la industria se ha librado hasta ahora de sufrir una catástrofe operativa importante, esta buena suerte podría acabarse si las empresas no se esfuerzan por mejorar sus programas de ciberseguridad.

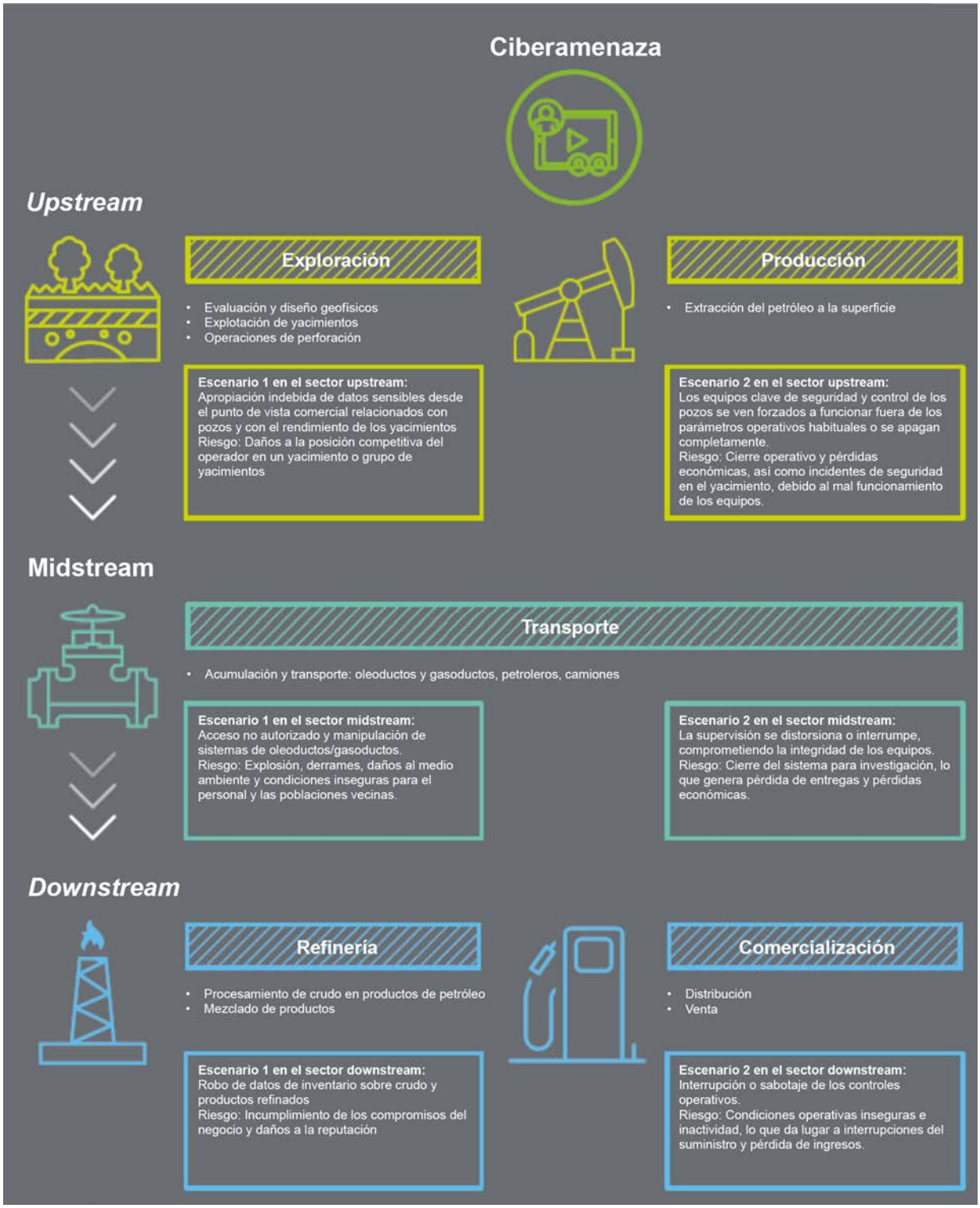
Hasta la fecha, las empresas de petróleo y gas se han centrado fundamentalmente en proteger lo referente a la propia empresa, en lugar de las operaciones, los sistemas y los datos. Esto se debe a que el concepto de Internet de las Cosas —donde la producción puedeser controlada desde un iPad o un *smartphone*, por ejemplo— es relativamente nuevo, si bien ha ido adquiriendo cada vez mayor impulso a lo largo de la última década. Asimismo, los sistemas operativos son intrínsecamente diferentes, y requieren tener conocimientos técnicos especializados y no solo experiencia en TI, para poder protegerlos de forma adecuada.

Actualmente, se necesita un enfoque que aúne tecnologías de la información e ingeniería para abordar la ciberseguridad de manera sostenible y a través de la programación. A continuación, se analizan los objetivos de un enfoque de estas características, así como los pasos prácticos para ponerlo en marcha.

En primer lugar, analicemos los tipos de ciberriesgo a los que se enfrenta el sector de los hidrocarburos, cómo pueden trastocar la cadena de valor y qué consecuencias podría tener.

Aunque la industria se ha librado hasta ahora de sufrir una catástrofe operativa importante, esta buena suerte podría acabarse si las empresas no se esfuerzan por mejorar sus programas de ciberseguridad.

Figura 1. Cómo afectan las ciberamenazas a la cadena de valor del gas y el petróleo



Análisis de los riesgos

Uno de los principales factores que hacen tan difícil proteger los ICS es que no se han diseñado para estar conectados; sin embargo, actualmente funcionan en red. La digitalización de los procesos operativos en el sector del petróleo y el gas ha dado lugar a nuevas oportunidades para mejorar la productividad y abaratar costes.

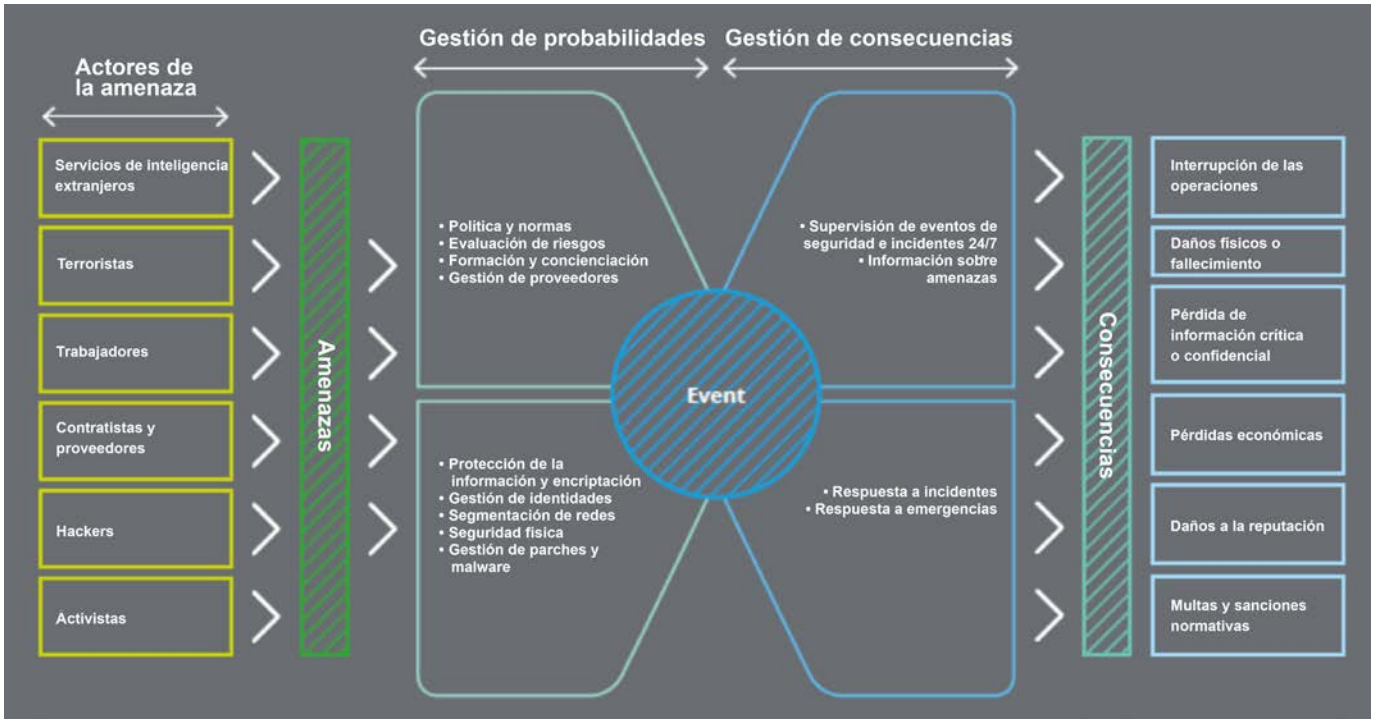
No obstante, la convergencia de los sistemas operativos y los sistemas empresariales también ha expuesto a la empresa a todo un nuevo mundo de ciberriesgos. Pensemos en los escenarios siguientes, cuya existencia no era posible hace unos pocos años:

- La comunicación mediante un acceso remoto inseguro permite a un ciberdelincuente secuestrar un sistema de control de procesos y llevar la producción a niveles peligrosos.
- Unas prácticas de seguridad insuficientes por parte de un contratista independiente pueden permitir a un virus migrar a un entorno de producción, lo que puede ocasionar el cierre de sistemas críticos de Supervisión, Control y Adquisición de Datos (SCADA, en sus siglas en inglés) y la creación de condiciones de trabajo inseguras.
- Una verificación inadecuada de los sistemas de TI antes de su implantación puede generar una caída del sistema, dando lugar a una interrupción o al cierre de las operaciones.
- La tecnología adquirida directamente por una planta, sin una comprobación y evaluación adecuadas, no se actualiza, e introduce una vulnerabilidad que permite a los miembros de una comunidad competidora conseguir acceso remoto a controladores lógicos programables (PLC, en sus siglas en inglés), dándoles de este modo la capacidad para interrumpir el proceso de producción cuando quieran.

Como muestran estos ejemplos, las ciberamenazas pueden venir de múltiples direcciones, como, por ejemplo, de actores internos intentando sabotear la producción, competidores buscando causar daños a la marca, o grupos externos, tales como activistas, que tratan de provocar el cierre de las instalaciones.

No todas las vulnerabilidades proceden de la propia tecnología; los aspectos relaciona-

Figura 2. Ejemplo de un análisis bow-tie de «ciberriesgos» para una empresa de gas y petróleo



dos con el comportamiento también entran en juego. Por ejemplo, a veces la falta de conciencia sobre la seguridad dentro de una organización puede exponer los sistemas a ciberataques de manera involuntaria, como cuando los empleados traen al entorno de trabajo medios portátiles que están infectados con *malware*. Por otro lado, muchos empleados creen simplemente que sus sistemas son un objetivo improbable, por lo que se muestran reacios a asumir la necesidad de cambiar de actitud e implantar nuevos protocolos de seguridad. Después de todo, no hace tanto que podían presuponer sin temor a equivocarse que todos los componentes de los equipos eran fiables, algo que ya no es así, puesto que los controladores y sensores digitales pueden ser manipulados para introducir datos falsos y confundir la información sobre el estado de los equipos. Otro supuesto que ya no puede darse por válido es que los fallos en los procesos se deben principalmente a condiciones atmosféricas, errores humanos o agotamiento de los equipos, y no necesariamente a la manipulación malintencionada del sistema por personas que tratan de causar un daño.

Tanto si un incumplimiento en materia cibernética es intencionado como si no lo es, las consecuencias pueden ser graves: desde comprometer datos confidenciales a desencadenar un fallo o una caída del sistema. Esto puede traducirse en una reducción de ingresos, daños a la reputación, catástrofes medioambientales, sanciones legales y, en casos extremos, pérdida de vidas humanas.

Es fácil ver por qué es necesario integrar de forma eficaz y exhaustiva los controles de ciberseguridad en los ICS, por no decir cada vez más imperativo. No obstante, para alcanzar esta integración, las empresas deben buscar la forma de conciliar los puntos de vista divergentes de las TI y las operaciones, ya que los especialistas en ICS no siempre comprenden los riesgos más novedosos para la seguridad de las TI, al igual que los expertos en seguridad de TI no suelen entender completamente el proceso industrial al que sirven de apoyo los ICS.

El análisis *bow-tie*, un concepto utilizado habitualmente en ingeniería para evaluar los modos de fallo, puede constituir una herramienta útil para salvar esta brecha. Aunque cada empresa llevará a cabo su análisis de manera específica, la figura 2 (pagina anterior) muestra un ejemplo de cómo un análisis *bow-tie* puede ser útil para una empresa de gas y petróleo.

La digitalización de los procesos operativos en el sector del petróleo y el gas ha dado lugar a nuevas oportunidades para mejorar la productividad y abaratar costes. No obstante, la convergencia de los sistemas operativos y los sistemas empresariales también ha expuesto a la empresa a todo un nuevo mundo de ciberriesgos.

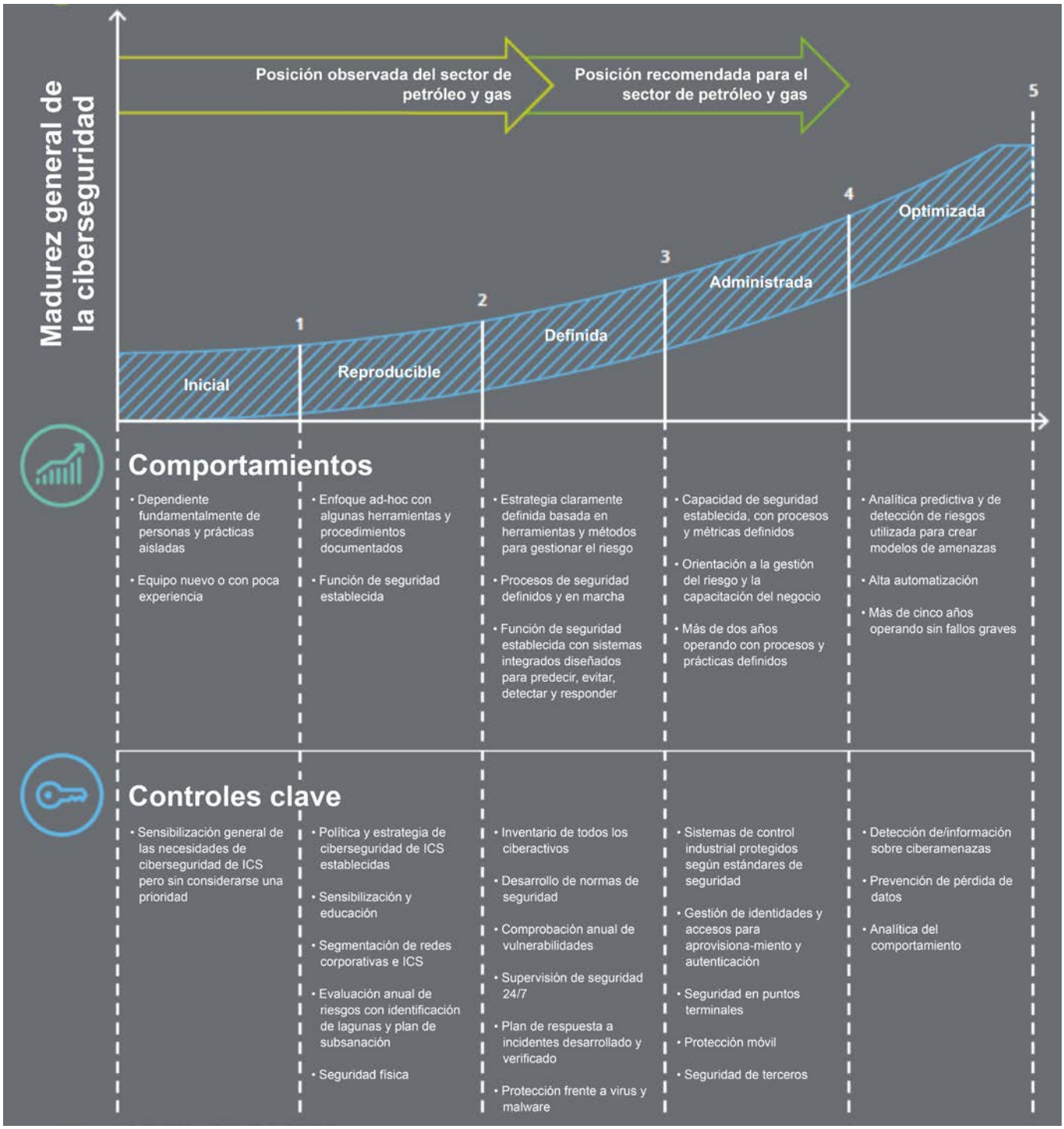
Evaluación del grado de madurez

Una vez que se entienden los riesgos, la empresa de gas y petróleo debe evaluar el grado de madurez de sus controles de ciberseguridad en un entorno operativo. Aunque no todos los riesgos pueden mitigarse, es importante saber qué tipo de controles están en marcha y dónde deben centrarse los esfuerzos de mejora. Esto supone prestar la debida atención a la forma en que los posibles incumplimientos en materia de seguridad dentro de los ICS se relacionan con los riesgos empresariales. Y lo que es muy importante, esto no puede hacerlo un grupo de TI o de ingeniería de manera independiente; se requiere un equipo multidisciplinar de profesionales de TI, ingeniería, operaciones y negocio para:

- **Realizar una evaluación del inventario de los activos e instalaciones y clasificarlos en términos de importancia.** Esto puede suponer plantearse preguntas tales como: ¿hay factores que pueden hacer de una instalación determinada un objetivo particularmente atractivo? ¿Se están aplicando los estándares de TI, los mecanismos de control y los procesos de supervisión a todos los activos ICS? ¿Se ha considerado toda la posible gama de cibervulnerabilidades y se han identificado las posibles consecuencias y cuantificado de manera adecuada?

- **Determinar si las instalaciones y activos críticos presentan vulnerabilidades bien conocidas y aprovechables.** En el sector del petróleo y el gas, estas vulnerabilidades difieren en cierto modo según el subsector. Por ejemplo, los sistemas de exploración están expuestos habitualmente al robo de datos protegidos, como estudios geofísicos, datos de exploración, estadísticas de pozos, trabajos de investigación e información sobre la planificación estratégica, todo lo cual puede poner en peligro el posicionamiento competitivo. Por otra parte, los sistemas de producción son vulnerables a la manipulación de los sistemas SCADA y otros sistemas operativos, así como a la pérdida de comunicación con las instalaciones en remoto y a las paradas de producción debido a infecciones por virus. En este aspecto, las consecuencias son más físicas, y pueden dar lugar a condiciones de trabajo inseguras y periodos de inactividad, lo que, a su vez, puede ocasionar pérdidas económicas y humanas. De igual modo, los ciberriesgos en el sector *midstream* también tienen consecuencias físicas y económicas, como condiciones inseguras, vertidos e interrup-

Figura 3. El modelo de madurez de ciberseguridad de Deloitte



ciones en el suministro o en el flujo de producción. El sector *downstream* también es vulnerable a la manipulación de los controles operativos, con las mismas consecuencias físicas y económicas que en los otros sectores. No obstante, este sector también abarca actividades de marketing de atención directa al cliente, lo cual da lugar a la posibilidad de que se produzcan robos de datos de clientes y se manipulen los sistemas comerciales. Esto podría generar pérdidas de ingresos, daños a la marca, e infracciones normativas y de cumplimiento.

- **Evaluar el grado de madurez del entorno de control para gestionar de forma proactiva estas amenazas.** Al evaluar la sofisticación de los procesos de gobierno y los controles, con frecuencia es útil utilizar un marco establecido, como el modelo de madurez en materia de ciberseguridad de Deloitte, que se presenta en la figura 3 (pagina anterior). Al llevar a cabo evaluaciones de madurez para una amplia gama de empresas de energía y recursos, hemos observado que el grado de madurez del sector de hidrocarburos en conjunto es aproximadamente de 2,5 en esta escala, mientras que la posición recomendada es por encima de 4.

Aunque no todos los riesgos pueden mitigarse, es importante saber qué tipo de controles están en marcha y dónde deben centrarse los esfuerzos de mejora.

A través del proceso de evaluación de la madurez, es importante entender la diferencia entre la seguridad para los sistemas empresariales y la seguridad para los sistemas de control industrial. En el actual entorno integrado, los estándares y procesos de seguridad de TI deben ser capaces de abordar tanto los sistemas de *back-office* como los sistemas ICS de una manera que no interfiera con los mecanismos existentes para garantizar la seguridad y la fiabilidad.

Además de la evaluación de la madurez, y como parte de las actividades de supervisión continuas, la necesidad de la organización de rastrear retroactivamente sus activos con regularidad no sólo para vigilar las vulnerabilidades conocidas, sino también para conocer las amenazas emergentes, las amenazas persistentes avanzadas (APT, en sus siglas en inglés), o los comportamientos sospechosos, e identificar los activos comprometidos antes de que se produzca un incidente.

Crear un programa unificado

Durante más de 50 años, la seguridad fue la principal motivación tras el diseño y la implantación de controles para procesos de producción físicos. Aunque esta motivación sigue presente para mantener los procesos en un estado operativo y seguro, ahora el conjunto de posibles interrupciones abarca también el terreno de lo cibernético. Esto requiere un programa unificado para poder abordar sistemáticamente la ciberseguridad en todas las operaciones y en el conjunto del negocio. Aunque crear e implantar un programa de esta naturaleza es una iniciativa de transformación que requiere varios años, cada fase de la iniciativa debería tener el mismo objetivo en mente: ascender en la escala de madurez para crear un entorno ICS que sea seguro, resistente y vigilante.

Seguro

La seguridad consiste en prevenir los incumplimientos o los hechos que puedan comprometer los sistemas mediante una supervisión y unos controles eficaces y automatizados. No obstante, no es posible asegurar todos los sistemas al mismo nivel. Las infraestructuras y activos críticos, y sus ICS asociados, estarían obviamente en cabeza en la lista, pero es importante recordar que no son componentes aislados. Forman parte de cadenas de suministro más amplias, de forma que es esencial reforzar los puntos débiles mediante procesos integrales. Esto puede implicar múltiples niveles y tipos de controles: desde crear sensores más sensibles en las instalaciones de procesamiento hasta instalar *firewalls*. Los sistemas deben diseñarse de forma que se tenga en cuenta que la entidad que explota un activo puede no ser la única organización con derechos sobre la información. Las empresas de servicios y suministros y los proveedores de equipos también pueden ganar una mayor visibilidad sobre los datos operativos y el rendimiento de los equipos a fin de mejorar los servicios que ofrecen. A menos que estén debidamente estructurados, esto podría dar lugar a fugas de datos imprevistas o deficiencias del sistema, que podrían ser aprovechadas por terceros. Por tanto, es esencial desarrollar sistemas de control y supervisión con derechos de acceso a los datos claramente definidos, así como capacidad para identificar cuando se infringen estos derechos.

Vigilante

La seguridad por sí sola no es suficiente. Debe ser acompañada de vigilancia, o de una supervisión continua, para determinar si un sistema sigue siendo seguro o se ha visto comprometido.

Para emprender iniciativas que refuercen la vigilancia y resulten eficaces, hay que empezar por saber de qué necesita defenderse la empresa. En el sector petrolero y gasístico pueden distinguirse varias tendencias

en cuanto a los tipos de amenazas, que ofrecen un buen punto de partida para entender las distintas clases de ataques que se están lanzando contra los sistemas ICS. Sin embargo, además de estas tendencias, la empresa necesita conocer sus riesgos de negocio específicos si quiere prever lo que podría ocurrir y diseñar sistemas de detección adecuados.

Resistente

Una organización resistente debe asegurarse de que cuenta con los planes y procedimientos necesarios para identificar un ciberataque, contenerlo o neutralizarlo, y para restablecer rápidamente las operaciones habituales. Estos procedimientos consisten en detectar, responder y recuperar, y los protocolos para garantizar un resultado de éxito dependerán del tipo de riesgo cibernético identificado.

En cualquier nivel de la cadena de valor del gas y el petróleo, ya sea en las operaciones *upstream* en boca de pozo, en las plantas de procesamiento *midstream* y en los oleoductos o gasoductos, o en la logística de refinería y distribución *downstream*, la supervisión continua y automatizada de los equipos debe permitir una detección en tiempo real de cualquier anomalía. Esto incluye saber en todo momento el estado de bombas, válvulas, compresores o unidades de procesamiento, incluidos los caudales y los patrones de fluidos y gases. Una visibilidad permanente sobre estas métricas debería facilitar una rápida reacción para eliminar los riesgos para la seguridad y el medio ambiente que provienen de operaciones fuera de control, llegando incluso al cierre de las operaciones cuando es necesario.

Es posible que sea difícil detectar una apropiación indebida o una alteración de datos sensibles desde el punto de vista comercial en relación con el rendimiento de los pozos, los caudales, o la utilización de los activos en entornos de procesamiento y refinería.

Por ello, es aún más importante crear salvaguardas en el diseño de estos sistemas de gestión de datos.

Incluso si los controles de seguridad fallan y tiene lugar un ciberataque sin que se haya detectado previamente, la capacidad para lanzar una respuesta contundente puede ayudar a contener las pérdidas de producción, al igual que los daños económicos, medioambientales y los daños a la marca. Las fases de respuesta y recuperación deberán incluir no solo la reparación inmediata de los equipos y sistemas comprometidos, sino también un análisis detallado de dónde y cómo se produjeron los ciberataques, qué vulnerabilidades del sistema permitieron que tuvieran lugar dichos ataques, y qué medidas de mitigación deben implantarse para evitar riesgos en el futuro.

Es fundamental entender que no basta con poner en marcha estrategias y políticas simplemente.

Al igual que en un simulacro de incendio corriente, las empresas deben ensayar periódicamente a través de simulaciones y juegos bélicos cibernéticos, en los que participen conjuntamente equipos empresariales y tecnológicos.

Aunque crear e implantar un programa de esta naturaleza es una iniciativa de transformación que requiere varios años, cada fase de la iniciativa debería tener el mismo objetivo en mente: ascender en la escala de madurez para crear un entorno ICS que sea seguro, resistente y vigilante.

Implantación de los controles clave

Aunque el perfil de riesgo y los niveles de madurez varían, existen algunos pilares comunes para la transformación a efectos del ciberriesgo en un entorno ICS con los que prácticamente toda empresa de gas y petróleo debe contar. Implantar estos controles clave puede servir de punto de partida para un programa personalizado encaminado a lograr seguridad, vigilancia y resistencia.

- Sensibilización: la conciencia sobre ciberseguridad debe fomentarse entre los profesionales de distintas categorías dentro de la organización, y se les debe formar y dotar de las herramientas adecuadas para que interactúen con los sistemas de manera segura y responsable.

- Control de accesos: los componentes de los sistemas ICS, incluido el *hardware*, las aplicaciones y las redes, están asegurados tanto física como lógicamente, y sólo se permite el acceso después de una autenticación y autorización formales.

- Seguridad de las redes: el acceso a redes por cable e inalámbricas dentro de un entorno ICS está limitado y asegurado de acuerdo con prácticas líderes de gestión de identidad y accesos, que incluyen la autenticación, el aprovisionamiento dinámico, vigilancia 24 horas al día, 7 días a la semana, y seguridad en puntos terminales.

- Medios portátiles: el uso de medios portátiles dentro del entorno ICS está restringido y es rastreado para evitar *software* malicioso.

- Respuesta a incidentes: las políticas y procedimientos de gestión de incidentes se desarrollan y verifican periódicamente.

Figura 4. Controles clave

	CONTROLES		SEGURO		VIGILANTE		RESISTENTE
Gestión de la ciberseguridad	Gestión de riesgos y cumplimiento	Protección de la información	Gestión del ciclo de vida de la información	Gestión de amenazas	Comprobación de la preparación ante ciberataques	Gestión de incidentes	Respuesta a incidentes de seguridad
	Políticas y normas		Encriptación	Analítica de seguridad	Supervisión de eventos de seguridad		Gestión de la continuidad del negocio
	Formación y concienciación	Gestión de identidades y accesos	Autenticación				
	Gestión de proveedores		Gestión de roles y derechos				
			Gestión del ciclo de vida de identidades				
		Protección de infraestructuras	Seguridad de redes				
			Seguridad física				
			Seguridad de sistemas				
			Parcheado y vulnerabilidad				
			Protección frente a malware				

Aunque el perfil de riesgo y los niveles de madurez varían, existen algunos pilares comunes para la transformación a efectos del ciberriesgo en un entorno ICS con los que prácticamente toda empresa de gas y petróleo

Adoptar prácticas de buen gobierno

Es esencial tener clara la responsabilidad con respecto a la seguridad de los sistemas ICS. Las funciones y responsabilidades deben estar claramente definidas para todos los implicados, desde los directivos a los operadores de procesos, o a terceras partes. En definitiva, debe haber una única línea de rendición de cuentas. Sin ella, será difícil no solo definir los requisitos que se aplicarán a todo el conjunto de la organización, sino también determinar si son adecuadas las soluciones centralizadas o locales.

En el pasado, el área de fabricación e ingeniería era la responsable del entorno de producción, incluidos los sistemas ICS y los mecanismos de seguridad asociados. Hoy día, la seguridad ICS es cada vez más una parte de la organización corporativa, y está bajo la supervisión del Director de Seguridad de la Información (CISO, por sus siglas en inglés). Sin embargo, no se trata de que el área de TI intervenga y dirija el yacimiento o la refinería. Aunque el CISO sea el responsable último, el área de ingeniería sigue teniendo que encargarse de desarrollar las soluciones adecuadas e implantarlas en las instalaciones.

Implantar un programa de ciberseguridad dentro de un entorno de ICS plantea además algunos desafíos adicionales en relación con la gestión del talento. El perfil de los puestos de trabajo a menudo requiere que las personas estén ubicadas en las plantas durante una serie de años. Si no se les proporciona una trayectoria profesional clara, pueden ocurrir dos cosas:

1. Que los profesionales de TI que se ven obligados a desempeñar una función de seguridad de ICS consideren que el programa es una actividad meramente complementaria y no contribuyan de forma activa.

2. Que los profesionales expertos en seguridad rápidamente alcancen sus metas en una de las plantas y busquen otra organización.

Lo ideal es que la empresa desarrolle un programa de concienciación para salvar la

brecha entre los profesionales de TI e ICS, así como una trayectoria profesional definida para aquellos que quieran especializarse en seguridad de ICS. Esta trayectoria suele empezar con un puesto de analista en planta básico, y avanzar hasta un puesto de seguridad global dentro de la organización.

Implantar un programa de ciberseguridad dentro del dominio de ICS plantea además algunos desafíos adicionales en relación con la gestión del talento. ■

Conclusión

En los últimos años, el sector petrolero y gasístico ha visto cómo se difuminaban en gran medida las fronteras tradicionales entre las TI y los sistemas ICS dentro de las empresas. Hoy día, la evolución continúa con la digitalización de los yacimientos de gas y petróleo. A medida que esta interconexión prosigue su avance, la frecuencia y sofisticación de los ciberataques hacen lo propio. No obstante, la mayor parte de las empresas no han seguido el ritmo en términos de preparación.

El punto de partida es la evaluación del grado de madurez de los controles de ciberseguridad. Ir más allá de las cuestiones de seguridad operativa tradicional para implantar un programa seguro, vigilante y resistente no es esencial solamente para que las empresas de gas y petróleo mejoren su capacidad para proteger la integridad de sus operaciones ante la creciente gama de ciberamenazas, sino también para lograr la excelencia operativa aprovechando los beneficios en términos de productividad que ofrece un entorno ICS digitalizado y plenamente integrado.

El llamamiento para salvar la brecha en lo que respecta al grado de preparación ante lo cibernético nunca ha sido más enérgico, y cada vez es mayor el número de personas concienciadas de la amenaza de la ciberdelincuencia y del impacto potencialmente desastroso que puede tener en las infraestructuras críticas.