QBE
At the heart of it

De los planos a las brechas de seguridad

La transformación digital está redefiniendo el riesgo cibernético en los proyectos de construcción e infraestructuras

Tres ideas clave:

1. Cómo el avance digital está ampliando la exposición a ciberataques en la construcción

2. Cómo los incidentes cibernéticos pueden afectar al desarrollo de una obra

3. Por qué la resiliencia cibernética tiene que cubrir toda la cadena de suministro

Introducción

La transformación digital está cambiando el sector de la construcción, pero la gestión del riesgo no siempre ha evolucionado al mismo ritmo. A medida que las organizaciones adoptan tecnologías conectadas y digitalizan la ejecución de los proyectos, surgen nuevas exposiciones tanto en sistemas corporativos como en entornos operativos, con interrupciones digitales que pueden tener consecuencias reales.

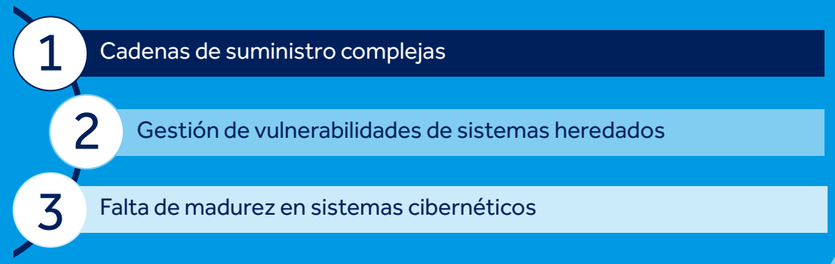
Los grandes proyectos de construcción dependen de cadenas de suministro complejas, plazos ajustados y herramientas digitales cada vez más interconectadas, y eso acaba generando vulnerabilidades importantes. Sistemas heredados, soluciones digitales implementadas con rapidez y conexiones de terceros poco protegidas pueden introducir debilidades que los actores maliciosos están explotando cada vez más. En paralelo, los reguladores están poniendo mayor foco en una gestión sólida del riesgo cibernético en sistemas de tecnologías de la información (IT), tecnologías operativas (OT)[1] y proveedores externos.

Además, el aumento de las tensiones geopolíticas está dando lugar a un incremento notable de los ciberataques dirigidos contra infraestructuras críticas y sectores estrechamente vinculados a ellas.

También están aumentando los riesgos derivados de la integración de los sistemas. Los ciberdelincuentes están aprovechando sistemas antiguos con medidas de seguridad insuficientes y la creciente conexión entre los entornos de IT y los sistemas operativos para causar el mayor impacto posible, ya sea con fines económicos o geopolíticos.

Las interrupciones en sistemas críticos o en proveedores pueden provocar paradas en los proyectos, conflictos contractuales, problemas de seguridad y consecuencias más amplias a nivel financiero, regulatorio y reputacional.

Figura 1: Los 3 principales riesgos digitales para el sector de la construcción según los expertos de Control Risks[2]

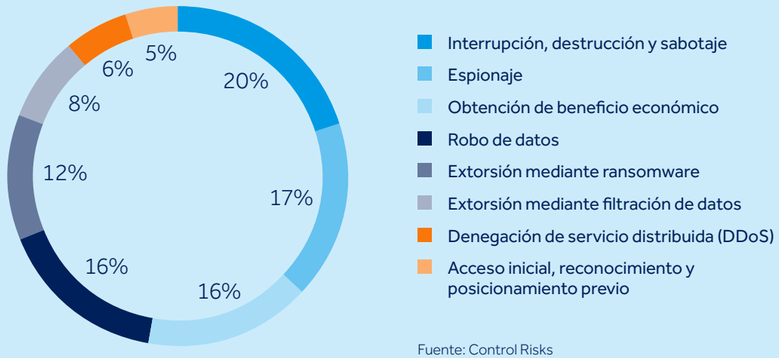


1 Tecnología operativa (OT): hardware y software que detecta o provoca cambios en el mundo físico mediante la supervisión y el control directo de dispositivos físicos, equipos o procesos industriales e infraestructuras.
2 Basado en una encuesta realizada a expertos senior de Digital Risks de Control Risks en las áreas de inteligencia de amenazas cibernéticas, asesoramiento en ciberseguridad y respuesta a incidentes.

La adopción de soluciones digitales y tecnologías emergentes aumenta la exposición cibernética

En los últimos años, el sector de la construcción ha acelerado la digitalización de sus operaciones. Las organizaciones están integrando cada vez más tecnologías emergentes como la inteligencia artificial (IA), dispositivos de Internet de las Cosas (IoT)[3] y herramientas específicas del sector, como Building Information Modelling (BIM).

Figura 2: Objetivos de los ciberincidentes dirigidos al sector de la construcción y a sectores adyacentes de infraestructuras críticas (porcentaje de incidentes significativos, 2023-26)



Fuente: Control Risks

La digitalización aporta beneficios claros: mejora la supervisión de la seguridad, refuerza el control del cumplimiento, automatiza procesos y hace más eficiente la ejecución de los proyectos. Por ejemplo, tecnologías como BIM permiten a los equipos colaborar en remoto sobre un mismo proyecto, asegurando que todas las partes trabajan con la misma información actualizada, como planos y modelos.

Sin embargo, la integración de nuevos sistemas digitales también amplía la superficie de ataque y genera nuevas formas de riesgo. Aunque la colaboración en la nube facilita la coordinación, estas infraestructuras son un objetivo frecuente para ciberdelincuentes y actores estatales que buscan robar información sensible o acceder a sistemas corporativos más amplios.

Estos mismos patrones de vulnerabilidad se observan en otras tecnologías cada vez más presentes en la construcción. Por ejemplo, un informe de 2025 señala un aumento interanual del 410 % en la actividad de malware dirigido a dispositivos IoT en el sector.[4] El uso continuado de sistemas heredados, la complejidad de las cadenas de suministro y los exigentes plazos de entrega siguen complicando la gestión del riesgo cibernético.

3 El Internet de las Cosas (IoT), o comunicación máquina a máquina (M2M), describe los miles de millones de dispositivos y equipos conectados a internet que se comunican entre sí con poca o ninguna intervención humana. Entre estos dispositivos se incluyen electrodomésticos, vehículos, tarjetas de crédito, ascensores y cámaras de videovigilancia (CCTV).
4 https://www.zscaler.com/resources/industry-reports/threatlabz-mobile-iot-ot-report.pdf

Los datos recientes del sector reflejan la magnitud de este cambio:

56 %

El 56 % de los inversores en construcción prevé aumentar la inversión en IA.[5]

61 %

El 61 % de los líderes del sector sitúa la tecnología y la innovación como prioridad estratégica.[6]

34 %

El 34 % de los profesionales participa en pruebas piloto de IA, y un 14,5 % ya la utiliza de forma habitual en uno o varios procesos de negocio.[7]

USD $17 72bn

El mercado global de BIM se valoró en 4380 millones de dólares en 2024 y se espera que alcance los 17 720 millones en 2034.[8]

En el sector de la construcción, los ciberataques ya no se limitan a comprometer la confidencialidad de la información; interrumpen la ejecución de los proyectos, paralizan las operaciones, tensionan las cadenas de suministro y ponen de manifiesto lo rápido que la dependencia digital puede convertirse en un riesgo operativo. Según avanza el sector en digitalización y automatización, las amenazas que surgen del entorno digital adquieren un carácter cada vez más crítico.

Socio de Digital Risks
Control Risks

5 https://www.rics.org/news-insights/artificial-intelligence-in-construction-report#
6 https://kpmg.com/dk/en/insights/market-trends/global-construction-survey.html
7 https://www.rics.org/news-insights/artificial-intelligence-in-construction-report#
8 https://finance.yahoo.com/news/bim-construction-industry-research-report-125300365.html

La extorsión y las tensiones geopolíticas impulsan los riesgos de interrupción en la construcción y las infraestructuras

79%

El 79 % de los expertos de Control Risks considera que el ransomware es la amenaza con mayor probabilidad de tener un impacto significativo en las organizaciones del sector de la construcción.

El sector de la construcción es especialmente vulnerable a la interrupción operativa. Los proyectos suelen ejecutarse con plazos ajustados y dependen de cadenas de suministro complejas, lo que hace que cualquier retraso se traduzca rápidamente en un aumento de costes y en consecuencias contractuales. Estas características incrementan la exposición del sector de la construcción a ataques de ransomware y extorsión, en los que la interrupción de la actividad se utiliza como principal herramienta de presión.

Según un estudio de 2023, el 77 % de las empresas del sector de la construcción empieza a sufrir graves problemas operativos si pasa más de cinco días sin acceso a la documentación de sus proyectos.[9] En 2025, los incidentes de ransomware provocaron una media de 24 días de inactividad.[10] En construcción, una interrupción de este tipo puede generar retrasos significativos, afectar a subcontratistas y proveedores, y causar un daño reputacional a largo plazo.

El coste de los incidentes de extorsión varía considerablemente según el caso, en función de factores como el grado de interrupción operativa o si se han sustraído datos sensibles. No obstante, existen referencias claras: en un incidente de extorsión por robo de datos en 2020 que afectó a una empresa con sede en Reino Unido, los costes de recuperación y asesoramiento alcanzaron los 7 millones de libras, a lo que se sumaron multas de 4,4 millones de libras impuestas por la autoridad británica de protección de datos.[11]

9 https://www.construction.com/reports/enhanced-data-resilience-will-help-the-design-and-construction-industry-face-the-risks-that-impact-their-businesses/
10 https://www.totalassure.com/blog/average-ransomware-recovery-time-2025
11 https://constructionmanagement.co.uk/poor-cyber-security-cost-interserve-11m-to-clean-up/

Caso Práctico

Operación de doble extorsión contra una empresa de construcción e ingeniería civil

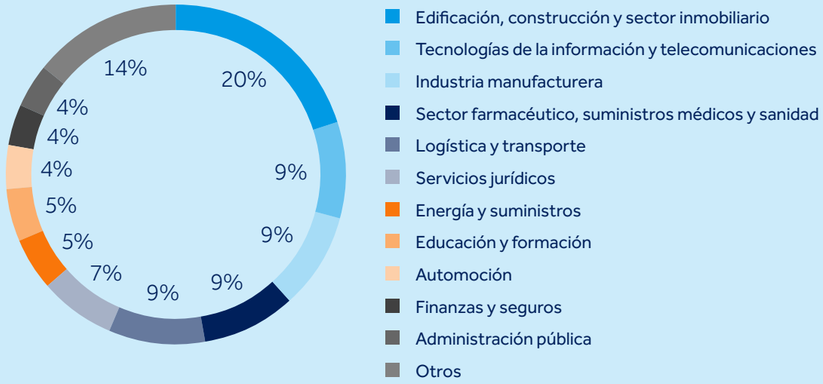
En febrero de 2023, la empresa británica de construcción e ingeniería civil Lagan Specialist Contracting Group (Lagan SCG) fue objetivo de una operación de doble extorsión. El ataque se atribuyó posteriormente a Lockbit, un grupo cibercriminal con una amplia experiencia en ataques de ransomware de gran impacto.

El incidente supuso el robo de una gran cantidad de datos sensibles de empleados, incluidos números de pasaporte y datos bancarios. Posteriormente, esta información se filtró en la dark web, exponiendo a los empleados a posibles fraudes. En mayo de 2023, se inició una demanda colectiva para investigar cómo se produjo la brecha de seguridad y cuál fue su impacto en la seguridad de los empleados.[12]

No hay constancia pública del impacto en Lagan SCG derivado del cifrado de sistemas. Sin embargo, pocas semanas antes, el mismo grupo atacó Royal Mail en un incidente similar que provocó una grave interrupción de sus operaciones. Según diversas fuentes, Royal Mail destinó 10 millones de libras a la recuperación y refuerzo de su resiliencia cibernética tras el ataque, lo que pone de manifiesto el impacto económico que puede tener un incidente de este tipo.

12 https://www.kpl-databreach.co.uk/lagan-specialist-contracting-group/

Figura 3: Sectores afectados por incidentes de ransomware en 2025[13]



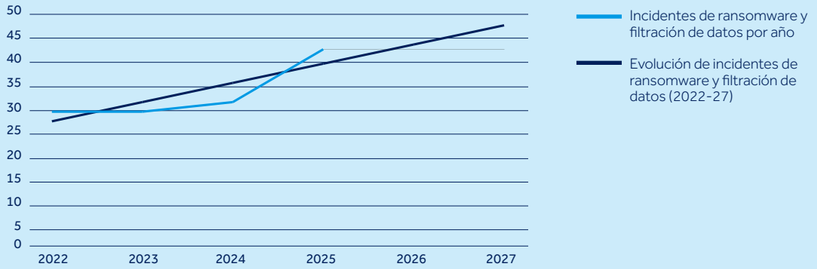
Fuente: Control Risks

Los grupos cibercriminales también están aprovechando la ampliación de la superficie de ataque en el sector. Conforme las empresas de construcción establecen conexiones remotas entre redes de contratistas y proveedores, por ejemplo, para facilitar sistemas BIM colaborativos, el número de posibles puntos de entrada para los atacantes se multiplica.

Al mismo tiempo, los actores de ransomware han mejorado su capacidad para atacar infraestructuras de tecnología operativa (OT). Un informe de ciberseguridad publicado en febrero señala que 119 grupos atacaron organizaciones industriales en 2025, lo que supone un incremento interanual del 49 %. En conjunto, estos grupos afectaron a 526 organizaciones del sector de la construcción, observándose una interrupción operativa significativa en todos los casos en los que el ransomware se desplegó en entornos OT.[14]

Cuando se introduce en infraestructuras OT, el ransomware puede interrumpir los sistemas de control industrial (ICS), software, hardware y redes especializadas que supervisan y controlan procesos industriales, provocando la parada de maquinaria física y limitando o incluso eliminando el control sobre sensores, sistemas de seguridad integrados y componentes como válvulas y bombas.

Figura 4: Operaciones de ransomware y extorsión mediante filtración de datos dirigidas al sector de la construcción y a sectores adyacentes de infraestructuras críticas (basado en incidentes significativos a nivel global, 2022-25)



Fuente: Control Risks

13 Los datos de Control Risks combinan incidentes dirigidos a los sectores de edificación, construcción y propiedad, incluyendo inmobiliaria, gestión de la propiedad y otros subsectores relacionados. Según estos datos, el ámbito de edificación, construcción y propiedad fue el principal objetivo de los incidentes de ransomware en 2025. Aunque el sector de la construcción ha sido uno de los principales objetivos de los actores de ransomware en 2025, estos resultados también se deben a un número significativo de incidentes dirigidos a entidades del sector inmobiliario y de la propiedad.

14 https://5943619.hs-sites.com/hubfs/312-Year-in-Review/2026/Dragos-2026-OT-Cybersecurity-Report-A-Year-in-Review.pdf?hsCtaAttrib=205683189348

Caso Práctico

Un ataque de doble extorsión afecta a una empresa de construcción e ingeniería civil[15]

En marzo de 2024, la empresa estadounidense Skender Construction fue objetivo de una operación de doble extorsión llevada a cabo por un actor no identificado.

Como parte del ataque, el grupo accedió y extrajo datos sensibles de más de 1000 personas. Entre la información sustraída se encontraban datos de pasaportes y números de la seguridad social, lo que incrementa el riesgo de fraude para las personas afectadas a corto y medio plazo.

El atacante también logró cifrar los sistemas de IT de Skender Construction. Sin embargo, la compañía contaba con copias de seguridad preparadas, lo que le permitió restaurar los sistemas con rapidez y limitar el impacto operativo del incidente.

15 https://www.constructiondive.com/news/skender-ransomware-attack-chicago-maine/712844/

Más allá de la ciberdelincuencia, desde 2024 se ha producido un aumento notable de incidentes cibernéticos disruptivos vinculados a actores alineados con estados, dirigidos a infraestructuras críticas nacionales en países occidentales.[16]

Estos incidentes suelen estar relacionados con tensiones geopolíticas más amplias, especialmente entre Rusia y los países miembros de la OTAN, así como con la evolución del conflicto entre Estados Unidos, Israel e Irán. En esta situación, los ciberataques forman cada vez más parte de estrategias de guerra híbrida.

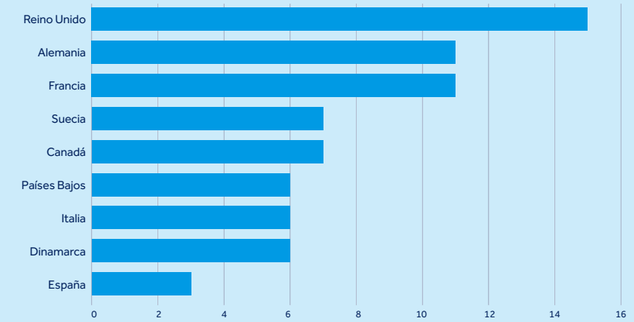
Aunque las empresas de construcción no suelen ser el objetivo principal de este tipo de operaciones, su proximidad a las infraestructuras críticas, por su papel en el diseño y construcción de activos físicos, las convierte en víctimas plausibles, tanto directas como colaterales. Por ejemplo, una empresa de construcción puede verse comprometida como parte de una cadena de ataque dirigida a un operador de infraestructuras críticas, o sufrir interrupciones derivadas de un incidente que afecte directamente a un proveedor o socio.

A medida que la construcción se vuelve más estratégica y ligada a infraestructuras clave, también aumenta el riesgo de ataques con motivación geopolítica, sobre todo si pueden frenar proyectos importantes. Es algo que se nota especialmente en países cercanos a zonas de tensión, donde algunos estados buscan impactar económicamente a sus rivales a través del ciberespacio.

Responsable global de inteligencia de amenazas cibernéticas en Control Risks

16 Control Risks

Figura 5: Número de incidentes disruptivos protagonizados por grupos alineados con estados cuyo objetivo son Canadá, Dinamarca, Francia, Alemania, Italia, Países Bajos, España, Suecia y el Reino Unido (incidentes significativos observados, 2022-26)



Fuente: Control Risks

Caso Práctico

Activista cibernético prorruso ataca infraestructuras hídricas

En 2024, el grupo prorruso Z-Pentest llevó a cabo un ciberataque destructivo contra una empresa de suministro de agua en Dinamarca. Tras acceder a los sistemas de control, manipuló los niveles de presión, provocando la rotura de al menos tres tuberías y dejando sin suministro a 500 hogares durante varias horas.[17]

En abril de 2025, el mismo actor atacó una presa en Noruega, abriendo válvulas de salida y liberando millones de litros de agua durante un periodo de cuatro horas, hasta que los operadores lograron recuperar el control del sistema. El ataque se atribuyó a contraseñas débiles en un panel de control accesible desde la web y a una falta de separación adecuada entre los sistemas OT y los sistemas IT conectados a internet.[18]

Desde entonces se han registrado incidentes similares, incluido un intento de ciberataque contra una instalación de agua en Polonia.[19] Estas operaciones forman parte de un patrón más amplio de actividad cibernética disruptiva dirigida a infraestructuras críticas. Aunque hasta ahora estos ataques se han centrado principalmente en servicios públicos y el sector energético, es probable que tácticas similares acaben afectando también a sectores adyacentes, como el de la construcción.

17 https://www.euronews.com/2025/12/19/denmark-blames-russia-for-cyberattacks-on-water-utility-and-election-websites
18 https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/
19 https://www.reuters.com/en/poland-foiled-cyberattack-big-citys-water-supply-deputy-pm-says-2025-08-14/

La convergencia entre IT y OT amplía la superficie de ataque y aumenta el riesgo operativo

A medida que avanza la digitalización, las empresas de construcción integran cada vez más los sistemas de IT con los entornos de OT. Cuando se implementa correctamente, esta convergencia de IT/OT puede optimizar las operaciones, facilitando la comunicación automatizada entre sistemas y mejorando la supervisión de los proyectos y los procesos clave.

Sin embargo, también incrementa el riesgo cibernético. Si la integración de los sistemas no es segura, un atacante que accede a la red de IT puede desplazarse lateralmente hacia los entornos OT sin ser detectado. Un informe de 2026 señala que una segmentación insuficiente entre sistemas IT y OT[20] fue un factor presente en el 81 % de los casos de respuesta a incidentes OT en 2025.[21]

Los riesgos derivados de una arquitectura insegura en la convergencia IT/OT se ven agravados por el uso continuado de infraestructura heredada, la concesión de accesos remotos privilegiados a terceros y prácticas de ciberseguridad deficientes, como la reutilización de credenciales.

Los actores maliciosos muestran un interés creciente en atacar directamente los sistemas OT. Desde 2024, se ha registrado un aumento de incidentes cibernéticos protagonizados por actores vinculados a estados que han atacado sistemas de control industrial (ICS) en el sector de servicios públicos en Europa y Norteamérica. Por su parte, los ciberdelincuentes también están dirigiendo sus ataques con mayor frecuencia a entornos OT. Un proveedor especializado en ciberseguridad OT informó de que el 23 % de los casos de respuesta a incidentes gestionados en 2025 implicaban ransomware dirigido a estos sistemas.[22] Muchos ataques siguen aprovechando puntos débiles en sistemas heredados. En 2025, el 67,5 % de los intentos de explotación se basaron en vulnerabilidades conocidas desde hacía tiempo.[23]

Dado que muchos sistemas OT dependen de software o hardware antiguo que no puede actualizarse fácilmente, esta tendencia supone un riesgo significativo. Explotando sistemas sin actualizar, los atacantes pueden obtener acceso inicial, moverse entre sistemas y, en última instancia, comprometer entornos operativos críticos.

A medida que los sistemas OT se convierten en un objetivo cada vez más atractivo para ataques cibernéticos disruptivos, el riesgo para las empresas de construcción aumenta. Además del impacto inmediato en la operativa y en la seguridad en la obra, estas interrupciones pueden generar pérdidas económicas importantes, conflictos contractuales, daños reputacionales a largo plazo e incluso consecuencias regulatorias.

20 Separación física o técnica insuficiente entre los sistemas de IT y la infraestructura OT, lo que facilita que un actor malicioso se desplace entre sistemas sin ser detectado y lleve a cabo actividades maliciosas tanto en entornos IT como OT. Por ejemplo, un sistema OT puede estar configurado de forma que permita una comunicación directa y no segura con sistemas corporativos de IT, como servidores de correo electrónico, lo que permitiría a un atacante utilizar un servidor comprometido para ejecutar comandos en el sistema OT.
21 https://5943619.hs-sites.com/hubfs/312-Year-in-Review/2026/Dragos-2026-OT-Cybersecurity-Report-A-Year-in-Review.pdf?
22 https://5943619.hs-sites.com/hubfs/312-Year-in-Review/2026/Dragos-2026-OT-Cybersecurity-Report-A-Year-in-Review.pdf?
23 https://medium.com/s2wblog/detailed-analysis-of-recent-trends-in-known-exploited-vulnerabilities-c81678a47f39

La presión regulatoria introduce nuevas exigencias en la gestión del riesgo cibernético

Figura 6: Los 3 principales factores que impulsan el interés por atacar al sector de la construcción según los expertos de Control Risks

1. Nivel bajo de madurez en ciberseguridad (percibido)
2. Complejidad en las cadenas de suministro y redes de terceros
3. Débil protección en edificios y sistemas inteligentes

Los reguladores están adoptando una visión cada vez más amplia de la ciberseguridad y la protección de las infraestructuras críticas (CNI). Marcos regulatorios como la Directiva actualizada de Redes y Sistemas de Información de la Unión Europea (NIS2), las previsibles actualizaciones de normativas equivalentes en Reino Unido y la propuesta canadiense Critical Cyber Systems Protection Act (CCSPA) establecen nuevas exigencias para las organizaciones que operan infraestructuras críticas y sus cadenas de suministro.

Es probable que estos requisitos regulatorios se trasladen a lo largo de toda la cadena de suministro, incluidas las empresas de construcción que participan en proyectos de infraestructuras.

Como consecuencia, las organizaciones del sector tendrán que adoptar un enfoque más estructurado, basado en el riesgo y centrado en la resiliencia para gestionar el riesgo cibernético. En la práctica, esto se traduce en reforzar la gobernanza, mejorar las prácticas de seguridad en entornos IT/OT y asegurar planes sólidos de respuesta ante incidentes.

Figura 7: Componentes clave de una gestión eficaz del riesgo cibernético

Gobernanza

- Implementar una gestión integral del riesgo cibernético
- Establecer supervisión y responsabilidad a nivel directivo

Respuesta ante incidentes

- Revisar y actualizar los planes de respuesta ante incidentes y de continuidad del negocio, garantizando el cumplimiento de los requisitos de notificación
- Realizar pruebas periódicas con escenarios reales

Gestión del riesgo en la cadena de suministro

- Evaluar el riesgo de proveedores
- Incluir la ciberseguridad como parte de los procesos de contratación

Medidas técnicas

- Actualizar los controles de seguridad, incluyendo la segmentación de redes entre sistemas IT y OT, herramientas de detección y respuesta en endpoints (EDR) y políticas de parcheo actualizadas
- Identificar los sistemas heredados y definir estrategias de mitigación para aquellos que no puedan seguir los ciclos habituales de actualización

Formación y concienciación

- Impulsar programas de concienciación en ciberseguridad para toda la plantilla
- Fomentar la notificación de actividades sospechosas

El punto de vista de suscripción

Javier Redondo
Head of Financial Lines, Cyber & Specialty Markets

Desde la suscripción ciber, y desde la experiencia de trabajar de forma recurrente con empresas del sector, la construcción es uno de los mejores ejemplos para entender cómo un incidente digital puede convertirse rápidamente en una interrupción del negocio.

La razón es sencilla: nunca se ha utilizado tanta tecnología ni de una forma tan interconectada. Sistemas informáticos, tecnología operativa, plataformas de terceros y cadenas de suministro digitales se combinan en tiempo real, y además en múltiples proyectos de manera simultánea. Esa complejidad, que aporta eficiencia y agilidad, también abre nuevas vías de exposición al riesgo.

En España, este escenario se desarrolla en un contexto cada vez más exigente. La entrada en vigor de la Directiva NIS2 y el refuerzo del marco nacional de ciberseguridad están elevando claramente las expectativas sobre cómo las empresas gestionan estos riesgos. Ya no se trata únicamente de evitar incidentes, sino de demostrar que la organización es capaz de seguir funcionando cuando algo falla. En la práctica, la resiliencia ciber empieza a tener un peso creciente en la relación con clientes, promotores y socios, e incluso a convertirse en un factor relevante a la hora de acceder a determinados proyectos.

Esta evolución se refleja también en el tipo de incidentes que estamos viendo en el mercado. Cada vez es más habitual que un ataque no se limite a un problema de datos o de privacidad. Lo verdaderamente crítico aparece cuando se interrumpe la operativa, se bloquea el acceso a sistemas clave o se generan impactos directos en procesos físicos a través de entornos conectados. En muchos casos, el mayor daño no es técnico, sino operativo y económico: obras paralizadas, retrasos acumulados y decisiones críticas que deben tomarse bajo una fuerte presión de tiempo. En construcción, hablar de riesgo ciber es hablar directamente de riesgo operativo.

Desde el punto de vista de la suscripción, y atendiendo a casos reales observados, llama la atención que muchos de los incidentes más graves no tienen su origen en ataques especialmente sofisticados. Con frecuencia están ligados a problemas bien conocidos: sistemas heredados difíciles de actualizar, una separación insuficiente entre entornos de IT y tecnología operativa, técnicas de ingeniería social o proveedores de confianza que, sin pretenderlo, acaban convirtiéndose en una vía de entrada para un atacante.

Trabajar de forma consistente sobre estos aspectos básicos marca una diferencia material. La correcta segmentación entre entornos de IT y OT sigue siendo una de las medidas más eficaces para limitar el impacto de un incidente. Lo mismo ocurre con disponer de visibilidad sobre sistemas legacy, corregir vulnerabilidades conocidas o invertir en formación para que las personas sepan identificar un correo de phishing o una llamada fraudulenta. Son medidas sencillas en apariencia, pero con un impacto claro en la reducción del riesgo.

No obstante, la gestión del riesgo ciber no termina en la prevención. La capacidad de responder de forma rápida y ordenada cuando ocurre un incidente es igual de crítica. Contar con planes de respuesta probados, estructuras claras de toma de decisiones y una visión realista de los tiempos de recuperación es clave para minimizar el impacto en la actividad. En este contexto, disponer de un programa de seguros bien estructurado, alineado con la realidad operativa del negocio y respaldado por un enfoque técnico sólido, se convierte en una pieza esencial dentro de la estrategia global de resiliencia.

Por todo ello, también están evolucionando las conversaciones con los corredores, con quienes cada vez trabajamos de forma más estrecha para trasladar este enfoque al cliente final. Las empresas muestran hoy menos interés por amenazas abstractas y más por cuestiones muy concretas: cuánto tiempo podrían estar paradas, cómo se verían afectados sus proyectos en curso y con qué rapidez podrían volver a la normalidad. En el sector de la construcción, este cambio de enfoque es especialmente relevante, porque en la práctica lo que se está asegurando cada vez más es el riesgo ciber y la interrupción del negocio como dos caras de una misma realidad.

Natalio García
Head of Construction

Desde la perspectiva de la suscripción en España, uno de los cambios más claros en el sector de la construcción, además de los nuevos materiales y métodos constructivos, es la rapidez con la que el riesgo ciber se ha convertido en un factor clave para la ejecución de los proyectos.

Los proyectos ya operan bajo una gran presión, con márgenes muy ajustados y modelos cada vez más complejos. En este contexto, cualquier interrupción resulta especialmente costosa. Cuando un incidente ciber bloquea el acceso a la información, dificulta la coordinación entre equipos o paraliza la obra, las consecuencias llegan rápidamente en forma de retrasos, conflictos y sobrecostes.

También están cambiando las expectativas a nivel regulatorio y de clientes. La creciente atención a la ciberseguridad, especialmente en sectores ligados a infraestructuras críticas y sus cadenas de suministro, está elevando el nivel de exigencia. En un sector tan conectado con el transporte, la energía o el agua, muchas empresas se ven afectadas directa o indirectamente. Para los corredores, la ciber resiliencia empieza a ser un aspecto habitual en las conversaciones con clientes, no solo desde el punto de vista del riesgo, sino como un requisito para acceder y mantenerse en determinados proyectos.

Desde suscripción, esto está haciendo que el riesgo ciber deje de verse como algo secundario y pase a considerarse un riesgo relevante, con impacto directo en los plazos y en el presupuesto de las obras.

En las conversaciones con clientes y corredores, cada vez ponemos más foco en los riesgos digitales dentro de la gestión global del proyecto. Si perder el acceso a sistemas, planos o modelos BIM puede retrasar una obra, ese escenario debería contemplarse junto al resto de riesgos críticos y contar con planes de contingencia claros. La adopción de BIM aporta eficiencia, pero también concentra posibles puntos de fallo, por lo que no basta con pensar solo en la prevención. Un ataque de ransomware puede prolongarse durante semanas y es clave saber cómo continuar la actividad o detenerla de forma segura.

Otro aspecto fundamental es la cadena de suministro. En construcción, el riesgo rara vez está concentrado en un único punto. La dependencia de subcontratistas, proveedores y plataformas digitales compartidas hace que la exposición esté distribuida, aunque las consecuencias no siempre lo estén. Además, los contratos a precio cerrado y las penalizaciones por retrasos pueden activarse rápidamente, independientemente de dónde se origine el incidente. Por eso, conocer el nivel de madurez en ciberseguridad de terceros es cada vez más importante.

En definitiva, el cambio es también de mentalidad. La ciber resiliencia no va solo de tecnología, sino de proteger la entrega de los proyectos. Aunque la cobertura ciber no suele estar incluida en las pólizas tradicionales de construcción, estos riesgos pueden abordarse de forma específica con el apoyo de aseguradoras especializadas. Iniciar estas conversaciones desde fases tempranas ayuda a entender la exposición y a gestionarla mejor en un entorno que no deja de evolucionar.

Encuesta

Como parte de este informe, hemos contado con la opinión de 20 expertos senior del área de Digital Risks de Control Risks sobre los principales riesgos y puntos débiles en el sector de la construcción e infraestructuras. En el análisis han participado profesionales de los equipos de Control Risks en EMEA, APAC y América, incluyendo Londres, Berlín, Copenhague, Hong Kong, Nueva York, Washington, Sídney y Bogotá.

La encuesta recoge las aportaciones de consultores con amplia experiencia, practice leaders, y la mayoría de los socios (Partners) de las áreas de Threat Intelligence, Cyber Advisory y respuesta a incidentes. Cuando en el informe se hace referencia a “los expertos de Control Risks”, se trata de conclusiones basadas en los resultados cualitativos y cuantitativos de esta encuesta.

Para más información puedes visitar nuestra página web **qbeespana.com**

QBE European Operations
QBE Europe SA/NV, Spain
Paseo de la Castellana
31 – 5ª Planta
28046 Madrid
España
+34 91 789 39 50

qbeespana.com

This report was produced by QBE with Control Risks.

QBE
At the heart of it

1220126/2605-ES