Securitas

Securitas

Risk Intelligence Center

INTREP: Amenazas globales a la infraestructura crítica – Medidas de resiliencia

Intelligence@securitas.com

Contenido

Metodología

Objetivo

El RIC utiliza la información recopilada tanto de fuentes abiertas (OSINT) como de fuentes cerradas, como la inteligencia humana (HUMINT), y la procesa y analiza antes de realizar la evaluación final y su distribución.

Niveles de Amenaza

NIVEL EVALUADO DE AMENAZA	
5 – CRÍTICO	Amenaza extrema de disrupción. Revise y responda de ser necesario
4 – ALTO	Nivel de disrupción alto. Considere tomar acciones apropiadas.
3 – MODERADO	Nivel de amenaza moderado. Mantenga la alerta, y considere precauciones.
2 – BAJO	Nivel de disrupción bajo. Esté alerta.
1 – MUY BAJO	Nivel de disrupción insignificante. Esté alerta.

Lenguaje de Probabilidad

Esta evaluación utiliza el lenguaje de probabilidad del Corporate Risk Management (CRM) para proporcionar una evaluación de la probabilidad de que se manifieste una amenaza, en función de la probabilidad, utilizando un porcentaje, fracción o proporción como referencia. Esto ayuda a proporcionar contexto y claridad, y ayuda a mantener un enfoque estandarizado.

LENGUAJE DE PROBABILIDAD							
TÉRMINO:	Remoto	Altamente Improbable	Improbable	Posible	Probable	Altamente probable	Casi certero
PROBABILIDAD:	0 - 4%	10 - 20%	25 - 35%	40 - 50%	55 - 75%	80% - 90%	95 - 99%

Inteligencia Prioritaria

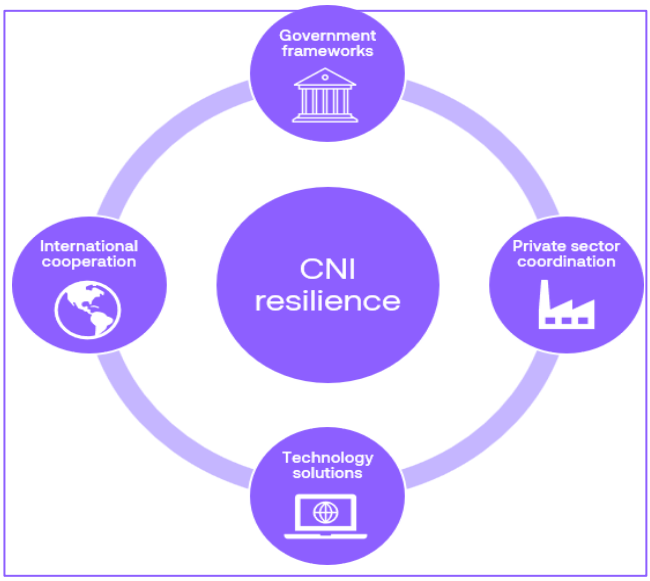
Fecha de corte de inteligencia	0800hrs UTC 29 julio 2025

NIVEL DE AMENAZA EVALUADO	
3 – MODERADO	Nivel de amenaza moderado. Mantenga la alerta, y considere precauciones.

- Las medidas de resiliencia de las infraestructuras nacionales críticas (INC) se están extendiendo a nivel mundial a través de marcos obligatorios, como la Directiva CER de la UE, la Ley KRITIS alemana y las autoridades ampliadas de la CISA estadounidense, pero su implementación sigue siendo inconsistente entre las distintas organizaciones.
- Los marcos normativos están convergiendo en requisitos comunes, entre los que se incluyen evaluaciones de riesgos, notificación de incidentes en un plazo de 24 a 48 horas y cumplimiento de las normas de ciberseguridad, aunque las organizaciones se enfrentan a limitaciones de financiación, vulnerabilidades debidas al envejecimiento de las infraestructuras y retos de coordinación entre el sector público y el privado.
- Las capacidades de resiliencia del sector privado varían significativamente entre regiones y sectores, y las economías desarrolladas muestran una mayor madurez en algunas industrias, pero siguen existiendo brechas en la resiliencia de la cadena de suministro y la coordinación intersectorial.
- Los incidentes graves ocurridos en 2025 demuestran que las organizaciones que cuentan con medidas de resiliencia proactivas, como redundancia, procesos operativos de respaldo y personal capacitado, obtuvieron mejores resultados en materia de recuperación, mientras que aquellas que dependían de puntos únicos de falla se enfrentaron a interrupciones prolongadas con efectos en cadena.
- EL Risk Intelligence Center (RIC) considera que es probable que las medidas de resiliencia de las infraestructuras críticas nacionales sigan siendo insuficientes frente a la evolución de las amenazas, y que las organizaciones que consideran la resiliencia como una prioridad estratégica, en lugar de un mero ejercicio de cumplimiento normativo, tengan muchas más probabilidades de dar respuestas más eficaces durante las interrupciones. Existe una posibilidad realista de que la inversión inadecuada del sector privado y la deficiente coordinación entre el sector público y el privado sigan exponiendo vulnerabilidades críticas, mientras que es muy probable que las organizaciones se enfrenten a un aumento de los costos de las interrupciones y a una prolongación de los tiempos de recuperación si no se invierte de forma proactiva en resiliencia.

Perspectiva general

La resiliencia de las infraestructuras nacionales críticas (CNI) se refiere a la capacidad de los sistemas esenciales para prepararse, absorber, recuperarse y adaptarse a eventos adversos, manteniendo al mismo tiempo las operaciones críticas. A diferencia de las medidas de seguridad básicas, que se centran en la prevención de incidentes, la resiliencia asume que se producirán interrupciones y hace hincapié en la rápida recuperación y la continuidad de las operaciones. Este enfoque integral aborda las amenazas cibernéticas, los desastres naturales, las interrupciones de la cadena de suministro y los fallos en cadena que pueden afectar a sectores enteros.



Elementos clave de resiliencia para la infraestructura nacional crítica (Fuente: RIC)

El entorno de amenazas global ha cambiado radicalmente la forma en que los gobiernos y las organizaciones abordan la protección de las CNI. Los actores estatales, los ciberdelincuentes, los activistas y los terroristas se centran cada vez más en las infraestructuras para lograr la máxima interrupción social, mientras que el cambio climático y las vulnerabilidades de la cadena de suministro crean nuevas categorías de riesgo. La convergencia de estas amenazas con el envejecimiento de las infraestructuras y la creciente digitalización ha creado un entorno de riesgo elevado que requiere enfoques sistemáticos de resiliencia.

Panorama de resiliencia

Los gobiernos han respondido con una intervención regulatoria sin precedentes, pasando de directrices voluntarias a requisitos obligatorios de resiliencia. La Directiva sobre la resiliencia de las entidades críticas (CER) de la UE, el marco KRITIS evolucionado de Alemania, la ampliación de las competencias de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) de EE. UU. e iniciativas similares en las economías desarrolladas representan la expansión más significativa de la regulación de las CNI en décadas. Estos marcos exigen evaluaciones de riesgos, notificación de incidentes, planificación de la continuidad del negocio y la implementación de normas de ciberseguridad reconocidas. La cooperación internacional se ha convertido en un componente fundamental, ya que las interrupciones de las infraestructuras traspasan cada vez más las fronteras y los sectores. Foros como el Critical 5 (Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos), los mecanismos de coordinación de la UE y las asociaciones bilaterales facilitan el intercambio de información, los ejercicios conjuntos y las respuestas coordinadas ante incidentes graves.

Las organizaciones del sector privado se enfrentan al complejo reto de traducir estos mandatos normativos en capacidades de resiliencia operativa. Esto implica no solo cumplir con una serie de requisitos, sino también introducir cambios fundamentales en el diseño, el funcionamiento y el mantenimiento de las infraestructuras. El panorama de la resiliencia presenta importantes variaciones regionales y sectoriales, tanto en los enfoques gubernamentales como en las capacidades del sector privado. Las economías desarrolladas, con marcos normativos sólidos e infraestructuras bien financiadas, muestran una mayor madurez en materia de resiliencia, mientras que las regiones en desarrollo suelen carecer tanto de marcos normativos como de recursos para su aplicación. Sin embargo, las economías complejas presentan sus propias vulnerabilidades, ya que dependen en gran medida de sistemas digitales que pueden sufrir graves perturbaciones en caso de crisis.

Marco de resiliencia gubernamental

Los gobiernos han implementado marcos normativos integrales que exigen medidas de resiliencia de la infraestructura crítica nacional, lo que supone un cambio significativo, pasando de ser directrices voluntarias a requisitos exigibles. Estos marcos establecen normas mínimas para la evaluación de riesgos, la notificación de incidentes, la planificación de la continuidad de las operaciones y la implementación de la ciberseguridad en todos los sectores críticos.

Europa y Norte América

UE Directiva de Resiliencia de Entidades Críticas (REC)

La Directiva CER, que entrará en vigor en octubre de 2024, amplió la regulación de las infraestructuras críticas nacionales (CNI) a 11 sectores críticos, entre los que se incluyen la energía, el transporte, la banca, la salud, el agua potable, las aguas residuales, las infraestructuras digitales, el espacio, la producción, el procesamiento y la distribución de alimentos, y los servicios postales. Los Estados miembros deben identificar las entidades críticas, exigir evaluaciones de riesgos en un plazo de nueve meses a partir de la notificación y garantizar medidas de protección adecuadas. Las interrupciones significativas del servicio deben notificarse en un plazo de 24 horas. Las autoridades también están facultadas para realizar verificaciones de antecedentes del personal sensible.

Marco KRITIS de Alemania

La Ley General KRITIS implementa la Directiva CER, y va más allá de la ciberseguridad para abordar la resiliencia física. El marco mantiene el umbral de 500 000 habitantes para la designación de instalaciones críticas y exige sistemas de detección de ataques de última generación. Los operadores de infraestructuras críticas deben informar de los incidentes a la Oficina Federal de Seguridad de la Información en un plazo de 72 horas.

Protección de la CNI de Reino Unido

El enfoque del Reino Unido está liderado por la Autoridad Nacional de Seguridad Protectora y el Centro Nacional de Ciberseguridad, con objetivos establecidos por el gobierno para que los operadores de CNI logren la resiliencia frente a los métodos de ataque comunes para 2025. El marco hace hincapié en la colaboración público-privada a través del Centro para la Protección de la Infraestructura Nacional (CPNI) y documentos de orientación específicos para cada sector.

Autoridades de la Agencia de Seguridad Cibernética y de Infraestructuras (CISA) de EE. UU

El Memorándum de Seguridad Nacional de abril de 2024 designó a la CISA como Coordinadora Nacional para la Seguridad y Resiliencia de Infraestructuras Críticas en 16 sectores de infraestructuras críticas. Las nuevas clasificaciones de «Entidades de Importancia Sistémica» identifican las infraestructuras de máxima prioridad. La Ley de Notificación de Incidentes Cibernéticos para Infraestructuras Críticas (CIRCIA) exige la notificación en un plazo de 72 horas, con sanciones que pueden alcanzar los 15 millones de dólares en caso de incumplimiento

Enfoques globales

Australia identifica más de 200 sistemas de importancia nacional a través de su Ley de Seguridad de Infraestructuras Críticas (SOCI), con obligaciones reforzadas que incluyen programas obligatorios de gestión de riesgos de infraestructuras críticas y el cumplimiento del marco de ciberseguridad. El marco abarca los sectores de las telecomunicaciones, la energía, el agua, el transporte y el almacenamiento de datos, y otorga al gobierno la facultad de emitir instrucciones durante los incidentes cibernéticos.

La Estrategia Nacional de Infraestructuras Críticas de Canadá establece asociaciones específicas para cada sector y requisitos de planificación de la resiliencia. La Política de Protección de Infraestructuras Críticas de Japón se centra en el intercambio de información y los mecanismos de respuesta coordinada. La Ley de Ciberseguridad de Singapur exige medidas de ciberseguridad para las infraestructuras de información críticas, con la obligación de notificar los incidentes en un plazo de dos horas.

Acciones Significativas (SIGACTs)

A continuación, se presenta una selección no exhaustiva de medidas recientes significativas (SIGACT) relacionadas con la legislación sobre resiliencia de la infraestructura crítica nacional.

Fecha	Ubicación	Estructura	Detalles	Impacto
Octubre 2024	UE	Iniciativa CER	Plazo de implementación para los Estados miembros.	11 sectores sujetos a requisitos obligatorios de resiliencia.
Abril 2024	EE. UU	Actualización NSM	CISA fue designada como Coordinadora Nacional.	Autoridades mejoradas en 16 sectores de la infraestructura nacional crítica.
Marzo 2024	Alemania	Ley KRITIS	Ley marco que implementa la iniciativa CER.	Mejorado de un enfoque exclusivamente cibernético a uno que abarca todos los riesgos.
Enero 2024	Australia	Actualización SOCI	Obligaciones reforzadas para entidades críticas.	Se identificaron 168 sistemas de importancia nacional.
Septiembre 2023	Reino Unido	Estrategia CNI	Estrategia de protección actualizada publicada.	2025: establecimiento de objetivos de resiliencia.
Julio 2023	Canadá	Estrategia CI	Implementación nacional de la estrategia.	Marcos de colaboración específicos por sector.

Implementación del sector privado

Los operadores de CNI están traduciendo los mandatos gubernamentales en capacidades de resiliencia operativa mediante enfoques sistemáticos de gestión de riesgos, continuidad del negocio, implementación de tecnología y seguridad de la cadena de suministro. La implementación varía significativamente en función de la madurez del sector, los recursos disponibles y los requisitos normativos.

Prioridades de resiliencia de la cadena de suministro

Las organizaciones han identificado las vulnerabilidades de la cadena de suministro como una brecha crítica en la resiliencia, especialmente tras perturbaciones importantes, como fenómenos meteorológicos extremos, interrupciones del transporte y tensiones

Ciclo de resiliencia del gobierno de Reino Unido (Fuente: gov.uk)

geopolíticas que afectan a proveedores clave. Las interrupciones de la infraestructura crítica nacional (CNI) se deben cada
vez más a las vulnerabilidades de los proveedores que a ataques directos a la infraestructura primaria. Las organizaciones implementan enfoques integrales que abordan la diversificación de proveedores, la evaluación de riesgos, la gestión estratégica de inventarios, la planificación de la redundancia, el intercambio de información y las soluciones tecnológicas que se describen a continuación

Las organizaciones avanzadas integran la resiliencia de la cadena de suministro con una planificación más amplia de la continuidad del negocio, estableciendo desencadenantes claros para activar proveedores alternativos y procedimientos de adquisición de emergencia. Las soluciones tecnológicas permiten supervisar en tiempo real la seguridad de los proveedores y enviar alertas automáticas sobre posibles interrupciones en las redes de suministro ampliadas.

Estudios de caso

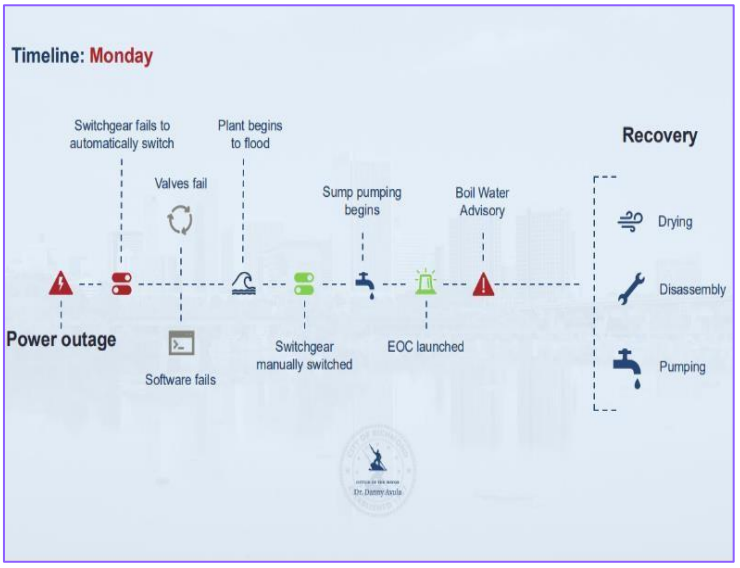
Amenazas medioambientales: Crisis del agua. Richmond, EE. UU (Enero 2025)

Detalles del incidente: Una tormenta de nieve provocó un corte de agua de seis días que afectó a cientos de miles de personas en Richmond, Virginia (EE. UU.), entre el 6 y el 11 de enero de 2025. La interrupción del suministro eléctrico en la principal planta de tratamiento de agua provocó fallos en cadena, entre ellos averías en los interruptores, válvulas de filtro atascadas e inundaciones en los sótanos que dañaron los equipos eléctricos.

Impacto: Corte de agua durante una semana, 68 roturas de tuberías principales tras la crisis, desvíos hospitalarios, cierres de escuelas y más de 20 000 citas médicas reprogramadas. No hubo compensación para los clientes a pesar de la interrupción del servicio.

Medidas de resiliencia implementadas: Las interconexiones regionales del sistema de agua permitieron a algunos condados aislar los suministros. Los preparativos previos a la tormenta incluyeron el abastecimiento de combustible a los generadores de respaldo y la declaración del estado de emergencia. La cooperación entre organismos facilitó la distribución de agua embotellada.

Deficiencias en la resiliencia: La planta funcionaba en "modo invierno" con una única fuente de energía, lo que creaba un punto crítico de fallo. Los generadores de respaldo no se activaron debido a la falta de personal eléctrico capacitado en las instalaciones. Las baterías de respaldo de los sistemas eran inadecuadas. La comunicación con el público se retrasó y fue inconsistentes.



Linea de tiempo del corte del servicio de agua en Richmond (Fuente: rva.gov)

Lecciones aprendidas: Los puntos únicos de falla resultaron devastadores. Los cambios posteriores al incidente incluyeron el funcionamiento permanente en «modo verano» con doble suministro de energía, protocolos de dotación de personal mejorados y 5 millones de dólares en mejoras de infraestructura. Esto demuestra la necesidad de realizar inversiones proactivas en lugar de respuestas reactivas ante las crisis.

Recomendación: Elimine los puntos únicos de falla en la infraestructura crítica mediante la implementación de fuentes de alimentación duales, sistemas de respaldo y la garantía de que se cuente con personal capacitado durante eventos climáticos extremos.

Sabotaje físico: Incidentes con cables submarinos en el Mar Báltico (Nov 2024 – Feb 2025)

investigación submarina del Gobierno finlandés sobre incidentes con cables

Detalles del incidente: Una serie de cortes en cables submarinos que afectaron a las conexiones de telecomunicaciones y energía entre Finlandia y Alemania, Lituania y Suecia, y Estonia y Finlandia. Se sospecha que se trata de un sabotaje perpetrado por buques, entre ellos el Yi Peng 3, de bandera china, y el Eagle S, vinculado a Rusia, con pruebas de arrastre de anclas en un tramo de hasta 160 km.

Impacto: interrupción mínima directa de internet debido a la redundancia, pero la repetición de ataques indica una amenaza persistente. El tiempo de reparación puede extenderse hasta 15 días por incidente. La UE comprometió alrededor de €1.000 millones para mejorar las capacidades de vigilancia y de reparación de emergencia.

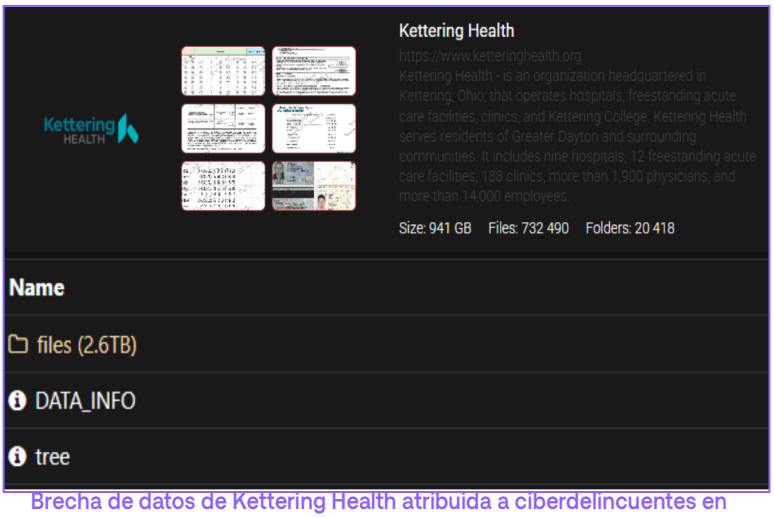
Medidas de resiliencia implementadas: las redundancias integradas en la red minimizaron las interrupciones en la conectividad a Internet. La OTAN lanzó la Operación Baltic Sentry en enero de 2025 para mejorar la vigilancia marítima. Los protocolos de respuesta rápida permitieron el decomiso de embarcaciones y la realización de investigaciones penales.

Brechas en la resiliencia: la persistencia de incidentes a pesar del aumento de la vigilancia sugiere una disuasión insuficiente contra los actores estatales. Las dificultades para atribuir la responsabilidad en aguas internacionales complican la respuesta diplomática. Las aguas poco profundas del Báltico hacen que los cables sean intrínsecamente vulnerables a daños deliberados.

Lecciones aprendidas: La redundancia de la red resultó fundamental para mantener la continuidad del servicio. Sin embargo, la resiliencia técnica por sí sola no es suficiente frente a la guerra persistente en la zona gris (GZW). Se necesita una mayor cooperación internacional y nuevos marcos jurídicos para lograr una disuasión eficaz.

Recomendación: Implementar una redundancia sólida de la infraestructura y participar en marcos de cooperación internacional para mitigar los riesgos derivados de ataques físicos patrocinados por Estados contra sistemas críticos.

Amenazas cibernéticas: Ransomware de Kettering Health, EE. UU (Mayo 2025)



Brecha de datos de Kettering Health atribuida a ciberdelincuentes en la dark web (Fuente: x.com/H4ckmanac).

Detalles del incidente: El grupo de ransomware Interlock atacó una red de 14 hospitales en Ohio el 20 de mayo, causando una interrupción del sistema de tres semanas. Los atacantes sustrajeron 941 GB de datos confidenciales, incluidos registros de pacientes, información médica y documentos financieros, lo que afectó a cientos de miles de personas.

Impacto: Interrupción del sistema que afectó a 14 hospitales y más de 120 centros ambulatorios. Se cancelaron las intervenciones quirúrgicas programadas, se desviaron las ambulancias durante una semana y se implementaron procesos manuales de atención al paciente. No se pagó ningún rescate, pero se incurrió en importantes costos de recuperación, incluidas responsabilidades legales y servicios de

monitoreo de crédito.

Medidas de resiliencia implementadas: respuesta inmediata ante incidentes, incluyendo segmentación de la red y aislamiento de servidores. Los protocolos para tiempos de inactividad permitieron que las salas de urgencias continuaran funcionando de forma manual. La colaboración con expertos forenses e ingenieros aceleró la recuperación.

Brechas de resiliencia: El éxito del despliegue del ransomware indica una ciberseguridad preventiva inadecuada. La filtración de datos demuestra el fracaso de la prevención de perdida de datos. La falta inicial de transparencia y el retraso en la comunicación sobre el alcance de la violación de la seguridad socavaron la confianza de los pacientes.

Lecciones aprendidas: La continuidad operativa es insuficiente si se compromete la privacidad de los datos. Los costos de recuperación son considerables, incluso sin pagar el rescate. Tras el incidente, se implementaron mejoras en la segmentación de la red, los controles de acceso y la supervisión. Es necesaria una resiliencia integrada que abarque tanto el tiempo de actividad como la integridad de los datos.

Recomendación: Desarrolle planes integrales de respuesta ante incidentes con segmentación de la red y procedimientos operativos manuales para mantener los servicios críticos durante los ciberataques y proteger al mismo tiempo los datos confidenciales.

Evaluación de inteligencia

Disrupción a infraestructura crítica (ataques cibernéticos, daño criminal, sabotaje, terrorismo)				
Tipo de Amenaza	Seguridad	Operación	Marca y Reputación	Nivel de Amenaza
Impacto:	3 – MODERADO	4 – ALTO	3 – MODERADO	3 – MODERADO

El Centro de Inteligencia de Riesgos (RIC) considera que las medidas de resiliencia de las infraestructuras críticas nacionales probablemente seguirán siendo insuficientes frente al panorama cambiante de amenazas, y que las organizaciones que tratan la resiliencia como una prioridad estratégica, en lugar de como un mero ejercicio de cumplimiento normativo, tienen muchas probabilidades de dar respuestas más eficaces durante las interrupciones. Existe una posibilidad realista de que la inversión inadecuada del sector privado y la deficiente coordinación entre el sector público y el privado sigan exponiendo vulnerabilidades críticas, mientras que es muy probable que las organizaciones se enfrenten a un aumento de los costos de las interrupciones y a una prolongación de los tiempos de recuperación si no realizan inversiones proactivas en resiliencia.

Es casi seguro que los marcos de resiliencia gubernamentales seguirán ampliándose, con la Directiva CER de la UE, la evolución de KRITIS en Alemania y la ampliación de las competencias de la CISA en Estados Unidos, lo que representa un cambio fundamental hacia normas aplicables. Sin embargo, existe una posibilidad realista de que la complejidad normativa y la superposición de requisitos generen cargas de cumplimiento sin mejoras proporcionales en materia de seguridad.

- La implementación en el sector privado varía significativamente en función de los recursos disponibles y la madurez normativa, y es probable que los sectores energético y financiero mantengan sus ventajas competitivas gracias a una planificación de la resiliencia superior. Es casi seguro que las organizaciones de estos sectores demostrarán una capacidad de recuperación más rápida debido a los marcos establecidos y a su mayor capacidad de inversión.
- Las empresas con operaciones en países menos desarrollados son muy propensas a sufrir interrupciones de las infraestructuras críticas debido a la menor calidad de las infraestructuras, las deficientes prácticas de mantenimiento y la menor resiliencia de la tecnología. Esto supone una amenaza para las empresas que intentan acceder a los mercados de los países en desarrollo, incluyendo amenazas medioambientales, delitos, conflictos y accidentes que pueden provocar cortes prolongados.

Los incidentes graves ocurridos en 2025 demuestran que las organizaciones que adoptan medidas proactivas de resiliencia obtienen resultados de recuperación notablemente mejores que las que se basan en enfoques reactivos. La crisis del agua de Richmond, los incidentes con los cables del mar Báltico y el ataque de ransomware a Kettering Health ponen de manifiesto la importancia de contar con infraestructuras redundantes, personal cualificado y una planificación exhaustiva.

- Las organizaciones que tratan la resiliencia como una prioridad estratégica, en lugar de como un mero ejercicio de cumplimiento normativo, es casi seguro que obtendrán mejores resultados durante las perturbaciones. Existe una posibilidad realista de que la inversión inadecuada del sector privado y la deficiente coordinación entre el sector público y el privado sigan poniendo de manifiesto vulnerabilidades críticas en las organizaciones que se centran exclusivamente en el cumplimiento normativo.
- Los conflictos actuales y las zonas de tensión probablemente sean indicadores de un aumento de los ataques contra las infraestructuras críticas nacionales debido al recrudecimiento de la guerra en la zona gris. Es casi seguro que zonas como el estrecho de Taiwán, el estrecho de

Ormuz y el mar Báltico seguirán sufriendo ataques de sabotaje contra cables submarinos y oleoductos, lo que afectará a las operaciones comerciales debido a la pérdida de conectividad.

Las interrupciones en las infraestructuras críticas nacionales (CNI) suponen una amenaza para las empresas de todo el mundo, por lo que es fundamental que las organizaciones evalúen no solo las CNI locales, sino también la calidad de las infraestructuras regionales y nacionales. Debido a la naturaleza integrada de los negocios con las CNI, muchos de los riesgos que plantean las interrupciones en las CNI son inevitables y supondrán una amenaza constante para las operaciones comerciales.

- Las empresas que pueden planificar para hacer frente a las interrupciones de las infraestructuras críticas nacionales (CNI) serán sin duda más resilientes, especialmente en las zonas menos desarrolladas del mundo, donde estas interrupciones son más frecuentes. El uso de evaluaciones de riesgos, incluidas las CNI locales, regionales y nacionales, puede ayudar a mitigar las amenazas mediante suministros eléctricos alternativos, comunicaciones de emergencia y activos operativos alternativos.
- Es muy probable que las infraestructuras críticas de comunicaciones altamente desarrolladas en Asia Oriental, Europa y América del Norte sean cada vez más objeto de amenazas cibernéticas debido a los avances en automatización y digitalización, mientras que las empresas tecnológicas que desarrollan operaciones digitales de infraestructuras críticas de comunicaciones constituyen objetivos directos para los ataques de interrupción.

Recomendaciones

Estratégicas / Operacionales

Para apoyar la toma de decisiones dinámicas en caso de una amenaza potencial (es decir, a un sitio, evento o persona), o en preparación para ella, a continuación, se presenta una lista de opciones estratégicas/operativas (es decir, medidas de planificación a nivel directivo) para consideraciones de seguridad y estratégicas. No se trata de una lista exhaustiva, y las organizaciones deben considerar los controles y medidas específicos de la organización y del sitio que sean pertinentes para su operación específica.

- Evaluar las dependencias de la infraestructura crítica nacional (CNI) de la organización mediante un mapeo exhaustivo de los proveedores críticos, los puntos únicos de falla y las dependencias intersectoriales.
- Implementar ciclos obligatorios de evaluación de riesgos y procedimientos de notificación de incidentes en un plazo de 24 a 72 horas, en consonancia con los marcos pertinentes, incluida la Directiva CER de la UE, los requisitos KRITIS o las autoridades CISA, en función de la jurisdicción operativa.
- Desarrollar programas integrales de resiliencia de la cadena de suministro, que incluyan la diversificación de proveedores, la clasificación basada en el riesgo, la gestión estratégica de inventarios y la supervisión continua de los proveedores con acuerdos con proveedores alternativos y procedimientos de adquisición de emergencia.

Táctico

A continuación, se incluye una lista de opciones tácticas y medidas de planificación para garantizar la seguridad en caso de una amenaza potencial (es decir, a un sitio, evento o persona) o como preparación para ella. No se trata de una lista exhaustiva, y las organizaciones deben considerar los controles y medidas específicos de la organización y del sitio que sean relevantes para su enfoque.

- Implementar procedimientos integrales de respuesta ante incidentes con funciones claramente definidas, segmentación de la red y capacidades de monitoreo las 24 horas del día, los 7 días de la semana.
- • Establecer capacidades sólidas de respaldo y recuperación, incluida una redundancia mínima N+1 para los sistemas críticos y la capacitación del personal en procedimientos de anulación manual.
- • Realizar pruebas de resiliencia periódicas mediante pruebas de comunicación mensuales, ejercicios de simulación trimestrales y simulaciones a gran escala anuales.
- • Mantener un inventario estratégico de componentes críticos con un stock mínimo de 30 días y una supervisión continua de la cadena de suministro.