



Plugged In

Revista de energía y servicios públicos

Primera edición

Artículos incluidos :

Del globalismo a la
seguridad nacional

ESG y seguridad cibernética son
dos caras de la misma moneda

Preparación para incidentes:
Un manual de estrategias
para su peor día

De la continuidad a la resiliencia



Contenido

03

Prefacio

05

Del globalismo a la
seguridad nacional

16

ESG y seguridad
cibernética son dos caras
de la misma moneda

23

De la continuidad
a la resiliencia

32

Preparación para incidentes:
Un manual de estrategias
para su peor día

38

KPMG's Global
Energy Institute



01

Prefacio

La descarbonización y la electrificación son tendencias gemelas que han llegado a definir los sistemas energéticos modernos. Como consecuencia de ello, la industria de energía y servicios públicos, en particular la generación de electricidad, está experimentando cambios drásticos. La energía renovable, tanto a escala de red como distribuida, junto con la revolución digital, altera la topología de la red y añade una complejidad colosal a la cadena de suministro de electricidad.

La conectividad digital también expuso las redes a ataques cibernéticos de *hackers* malintencionados y bandas criminales. Entre una creciente lista de incidentes se encuentra un asalto presuntamente patrocinado por el Estado a la red eléctrica de India por medio de dispositivos IoT y cámaras¹ y un intento de envenenamiento del sistema de tratamiento de agua de Florida²

Los fenómenos meteorológicos relacionados con el clima, como los incendios, las inundaciones, los vientos y el calor y el frío extremo, son una amenaza adicional que acentúa las vulnerabilidades de los activos envejecidos y aumenta el espectro de las demandas por daños al medioambiente y a las personas.

Todo ello se produce en un momento en el que la industria se enfrenta a un aumento de la demanda a medida que el mundo se recupera de la disrupción causada por la COVID-19, junto con los altos precios de la energía y las materias primas agravados por la guerra en Ucrania. Las expectativas de los clientes cambian rápidamente, y los consumidores buscan nuevos canales de participación digital al mismo tiempo que se convierten en proveedores de la red mediante la autogeneración.

No es exagerado decir que la electricidad es la base de casi todas las facetas de la vida moderna, sin la cual nuestra existencia diaria se ve amenazada. Para prestar el servicio 24 horas al día, los 7 días de la semana, que demanda la sociedad, los proveedores de energía y servicios públicos deben seguir siendo solventes, eficientes y seguros en un mercado volátil con altos costos de capital y mantenimiento y escasez de talento. Además, los reguladores exigen más a la industria de energía y servicios públicos que demuestre que ha hecho todo lo posible para evitar los cortes de suministro.

En esta primera edición de la revista *Plugged In*, analizamos cómo las empresas pueden hacer frente a los crecientes niveles de riesgo en la industria de energía y servicios públicos para seguir siendo resilientes y continuar impulsando a las personas, organizaciones y naciones.

Del globalismo a la seguridad nacional analiza cómo el conflicto en Ucrania cambió las nociones de las cadenas de suministro de energía mundiales, además de examinar las formas de abordar este y otros riesgos como la cibernética, la distribución, la inversión y la gestión de activos.



Anish De

Líder global de la industria de Energía y Servicios públicos, líder nacional de KPMG en Energía, Recursos naturales y Productos químicos, KPMG en India

¹ Business Standard, Suspected Chinese hackers collect intelligence from India's power grid, abril de 2022

² CNN, Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says, febrero de 2021

En **ESG y seguridad cibernética son dos caras de la misma moneda**, argumentamos cómo la confianza en las fuentes de energía renovable puede impulsar la revolución de la descarbonización, al superar las amenazas causadas por los ataques cibernéticos en una red distribuida.

Otro artículo, **De la continuidad a la resiliencia**, traza el cambio de enfoque de “respuesta y recuperación” a “resiliencia por diseño” para mantener los servicios las 24 horas del día, los 7 días de la semana por medio de estrategias como el fortalecimiento de la infraestructura, la modelización de fenómenos meteorológicos, la seguridad cibernética mejorada y el acceso a las habilidades adecuadas.

El cuarto y último artículo, **Preparación para incidentes: un manual de estrategias para su peor día**, adopta una visión realista de las diversas amenazas y considera cómo los proveedores de energía y servicios públicos pueden estar atentos a los riesgos para, en primer lugar, prevenirlos y, en el caso de que suceda lo peor, estar completamente preparados para minimizar las consecuencias.

La tecnología desempeñará un papel cada vez más importante en el riesgo y la resiliencia, con la automatización, la inteligencia artificial (IA), el internet de las cosas (IoT) y la realidad virtual/realidad aumentada (VR/AR), que ayudan a simular el impacto de futuros ataques y fenómenos meteorológicos, aumentar el control y la supervisión de las redes, identificar las infracciones, adaptarse rápidamente y activar la recuperación. Es probable que 5G esté en el centro de estos esfuerzos, mientras que el metaverso emergente puede abrir nuevas oportunidades para probar, comunicar y aprender nuevas capacidades.

Es un momento emocionante pero desafiante para la industria de energía y servicios públicos, y los profesionales de KPMG están trabajando con clientes a la vanguardia para ayudar a impulsar el futuro.

¡Disfruta de los artículos!



02

Del globalismo a la seguridad nacional

La evolución de los riesgos en la industria de la energía y los servicios públicos

Por: Valérie Besson, Anish De, Robert Johnston, and Stefano Moritsch



La guerra en Ucrania alteró drásticamente la percepción de la seguridad energética y aceleró la agenda de descarbonización de muchos países.

Desde que los tanques cruzaron la frontera ucraniana, muchos proveedores de energía y servicios públicos tuvieron que repensar sus estrategias de suministro de energía. Habiéndose acostumbrado a un mercado mundial dictado principalmente por el precio, la industria se adapta ahora a la idea de abastecerse de energía solo de países considerados aliados políticos.

La Unión Europea (UE) se comprometió a reducir en dos tercios su suministro de gas procedente de Rusia para finales de 2022, acordó una prohibición parcial del petróleo ruso¹ y anunció un acuerdo para comprar 15.000 millones de litros cúbicos adicionales de GNL (gas natural licuado) a EE. UU. para reducir su dependencia de la energía rusa². En cierto modo, los imperativos geopolíticos empujan ahora a la UE a acelerar drásticamente su ambición de cero neto, como lo demuestra su plan RePower EU.³ Incluso las regiones menos dependientes de las importaciones rusas para impulsar sus economías seguirán sintiendo el efecto de la volatilidad de los precios

mundiales de la energía a raíz de la dislocación del suministro, las sanciones occidentales, así como la auto-sanción por parte de las empresas que se cuidan de los daños a su reputación, un claro recordatorio de la importancia de cadenas de suministro de energía estables y resilientes.

Además de buscar nuevos proveedores de energía convencional, los gobiernos, especialmente en Europa, impulsarán una mayor eficiencia energética, acelerarán la transición a las energías renovables e invertirán en energía nuclear.

La industria de energía y servicios públicos ya estaba sufriendo una enorme perturbación antes de la guerra, con el cambio de la sociedad hacia todo lo eléctrico, la revolución de la energía verde que remodela las redes y la digitalización que afecta las formas de trabajo. Si a esto se añade la evolución de los riesgos geopolíticos, de la cadena de suministro, medioambientales, de inversión, cibernéticos, de talento y de costos, las compañías deben hacer frente a un futuro incierto.

“
Habiéndose acostumbrado a un mercado mundial dictado principalmente por el precio, la industria ahora se adapta a la idea de abastecerse de energía solo de países considerados aliados políticos.”



¹ Bruegel, Europe's Russian oil embargo: significant but not yet, junio de 2022

² BBC, EU signs US gas deal to curb reliance on Russia, marzo de 2022

³ European Commission, REPowerEU: A plan to rapidly reduce dependence on Russian fossil fuels and fast forward the green transition, mayo de 2022

Riesgo geopolítico/de la cadena de suministro: reescribiendo el mapa energético mundial

Una consecuencia de la desvinculación de la energía rusa podría ser la división del mundo en nuevos bloques energéticos de países que simpatizan ampliamente entre sí, como el Atlántico (EE. UU. y Europa), y China, India y Rusia, con el Golfo y otros países no alineados abasteciendo posiblemente a ambos bloques (a menos que las sanciones secundarias se conviertan en una opción).

Esta medida cambiaría radicalmente las cadenas de suministro mundiales, ya que los proveedores de energía y servicios públicos buscarían fuentes alternativas inmediatas, incluido el GNL de EE. UU. y otras regiones, para satisfacer la demanda interna de los consumidores y de las industrias que hacen un uso intensivo de la energía como la siderúrgica, la manufacturera y la de productos químicos.

Es probable que las cadenas de suministro de componentes nucleares,

de hidrógeno y de energía renovable, especialmente el uranio, las baterías y la energía solar y eólica, sufran una mayor presión a medida que se intensifique la carrera por las alternativas.

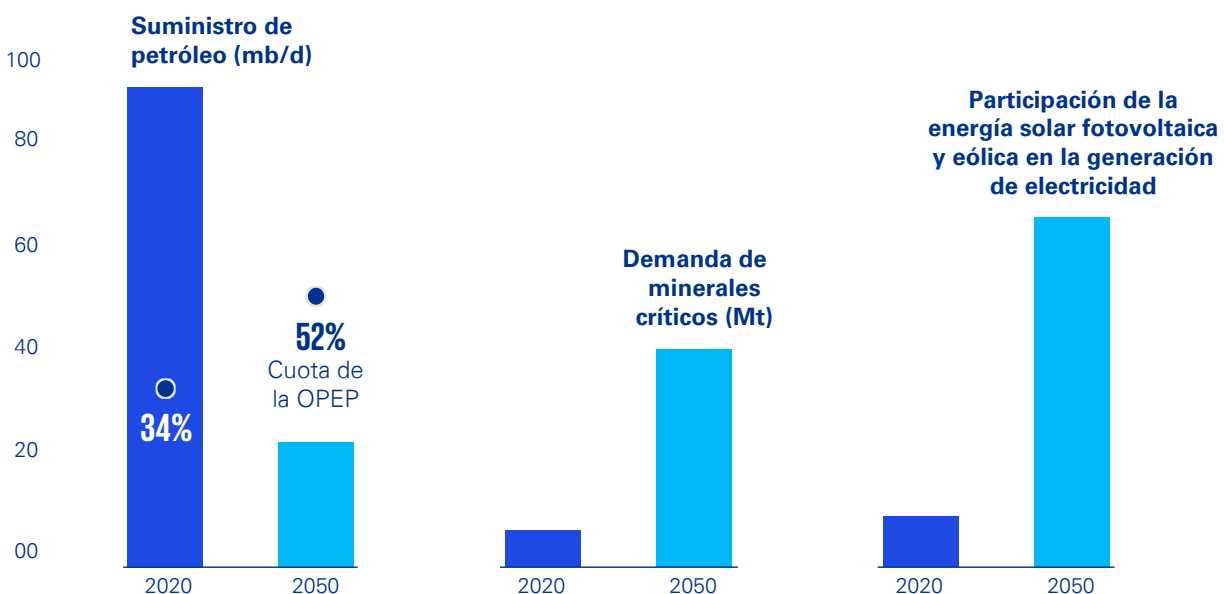
COVID-19 ya había expuesto las vulnerabilidades de las cadenas de suministro interdependientes a nivel global a medida que los actores de energía y servicios públicos luchaban por acceder a los recursos críticos durante la pandemia. Ahora que Rusia, Ucrania y posiblemente otros países vecinos quedaron efectivamente fuera de las cadenas de suministro, es vital encontrar rápidamente fuentes nuevas y confiables.

Los países que se encuentran en una etapa más temprana de su transición energética enfrentan decisiones difíciles, ya que tienen menos alternativas a los combustibles fósiles y no querrán arriesgarse a sufrir apagones o interrupciones industriales.



Acción: Defina los riesgos clave para la huella de su organización, monitoree eventos y planifique escenarios que abarquen diferentes resultados electorales, desarrollos de seguridad y tendencias ideológicas nacionales. Si es posible, estudie la posibilidad de proteger las cadenas de suministro de los riesgos duplicándolas en bloques regionales/ideológicos afines para limitar la exposición a la incertidumbre geopolítica.

Indicadores mundiales de seguridad energética en el camino hacia el cero neto



Nota: mb/d = millones de barriles por día; Mt = millones de toneladas.

Fuente: IEA, Net Zero by 2050: A Roadmap for the Global Energy Sector, May 2021

Riesgo de inversión: un impulso a la descarbonización

Para algunos gobiernos, especialmente en Europa, el impacto de reducir la dependencia del gas ruso y, en menor medida, del petróleo, ha hecho que estén aún más decididos a descarbonizar sus economías. La propuesta “Fit for 55” de la UE (para reducir las emisiones de gases de efecto invernadero en 55% para 2030) sigue siendo un importante motor de la inversión. China se comprometió a reducir su huella de carbono, con los consiguientes costos asociados a corto plazo.

Estados Unidos también tiene planes ambiciosos en materia de energía limpia. Sin embargo, con sus abundantes suministros de gas y petróleo de esquisto, seguirá siendo un actor importante en el mercado de los combustibles fósiles. Australia se ha visto relativamente poco afectado por los acontecimientos en Europa y tiene ricas reservas de carbón, gas y otros recursos naturales. Pero también tiene una agenda verde sólida, con muchos proyectos solares y eólicos en progreso.

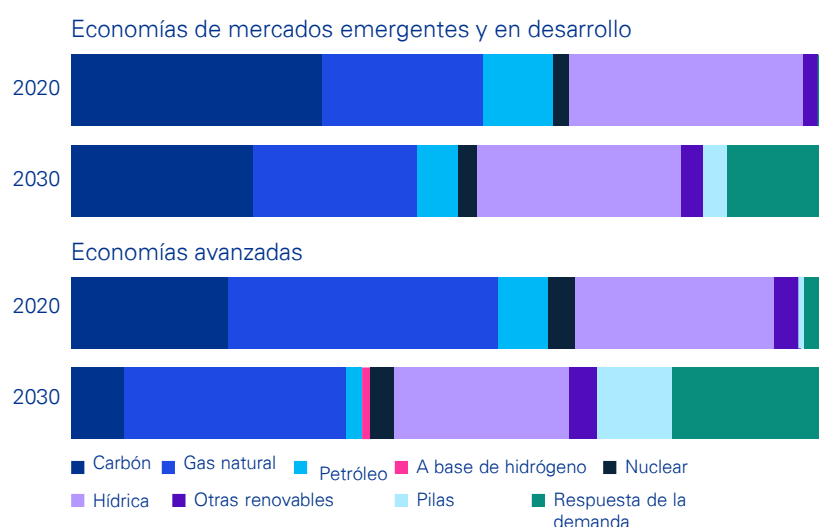
Casi un tercio de la electricidad de Australia en 2021 procedió de fuentes renovables, lo que supone un aumento del 5% con respecto al año anterior⁴. Los objetivos de cero neto ejercen una presión considerable sobre los gobiernos y los operadores privados de energía y servicios públicos para que inviertan en tecnologías libres de carbono. Es una historia similar con el renacimiento anticipado de la energía nuclear, que se espera que desempeñe un papel más destacado en la combinación de las fuentes de energía. El establecimiento de capacidades energéticas seguras requiere una amplia gama de infraestructura intensiva en capital para lograr la electrificación del transporte y otras partes de la economía. Estos esfuerzos se realizan principalmente país por país en lugar de iniciativas transfronterizas colectivas, por lo que las diferentes naciones avanzan a distintas velocidades.

La enorme inversión necesaria para lograr el cero neto puede poner a prueba a las economías que recién empiezan a salir de una recesión inducida por una pandemia.



Acción: En el ámbito de la industria, los proveedores de energía y servicios públicos deben trabajar para alcanzar sus objetivos de descarbonización organizacional, reducir las emisiones y elaborar informes ESG sólidos para demostrar que van por buen camino. Las empresas reguladas deben alinear sus objetivos con las últimas regulaciones o, alternativamente, buscar la aprobación cuando exista ambigüedad, si las regulaciones lo permiten (como es el caso en ciertas jurisdicciones). En el caso de las compañías que operan en segmentos no regulados o en los que no se dispone de una cobertura normativa directa, el abordaje adecuado es buscar instrumentos de financiamiento que se adapten explícitamente a sus circunstancias. El financiamiento de la transición está recibiendo mucha atención, ya que las autoridades reguladoras y los financiadores abordan explícitamente las necesidades de la transición y asumen los riesgos asociados. De esta manera, pueden obtener un grado de cobertura para sus riesgos de inversión.

Flexibilidad del sistema eléctrico por fuente 2020 y 2030⁵



⁴ Clean Energy Council, Clean Energy Australia Report, abril de 2022

⁵ IEA, Electricity system flexibility by source in the Net Zero Scenario, 2020 and 2030, octubre de 2021

Riesgo cibernético: amenazas crecientes en un área vasta para los ataques

Los activos de energía y servicios públicos se reconocen cada vez más como vitales para la seguridad nacional. Dadas las sanciones y otras acciones tomadas contra Rusia, y el apoyo a Ucrania, la amenaza de represalias es excepcionalmente alta en forma de *hacking*, *ransomware* y *malware*. Esto se suma a otros actores del estado-nación, delincuentes cibernéticos y *hacktivistas*. La escala geográfica y la complejidad de las organizaciones de energía y servicios públicos significan que las áreas de ataque son amplias, con el riesgo de poner fuera de servicio centrales eléctricas, generadores y turbinas eólicas; de desconectar redes de forma remota para detener la transmisión y distribución a los clientes; y de ataques al IoT, a los dispositivos y a los vehículos eléctricos, lo que lleva al robo de información del cliente, fraude en la facturación y a la interrupción de los servicios.



Acción: Para estar completamente preparados, los proveedores de energía y servicios públicos deben revisar sus planes de continuidad comercial, evaluar las vulnerabilidades a lo largo de la cadena de suministro y realizar ejercicios para recuperarse después de una infracción. Desarrollar una cultura de conciencia cibernética ayudará a evitar la posibilidad de un ataque y mejorará la notificación de incidentes. Y con las crecientes expectativas regulatorias, el monitoreo y la presentación de informes formales se han convertido en una gran prioridad. Dada la posibilidad de que se produzcan ataques por parte de estados-nación, la industria de energía y servicios públicos en su conjunto debe trabajar con el gobierno para reforzar las defensas y mejorar la capacidad de respuesta.



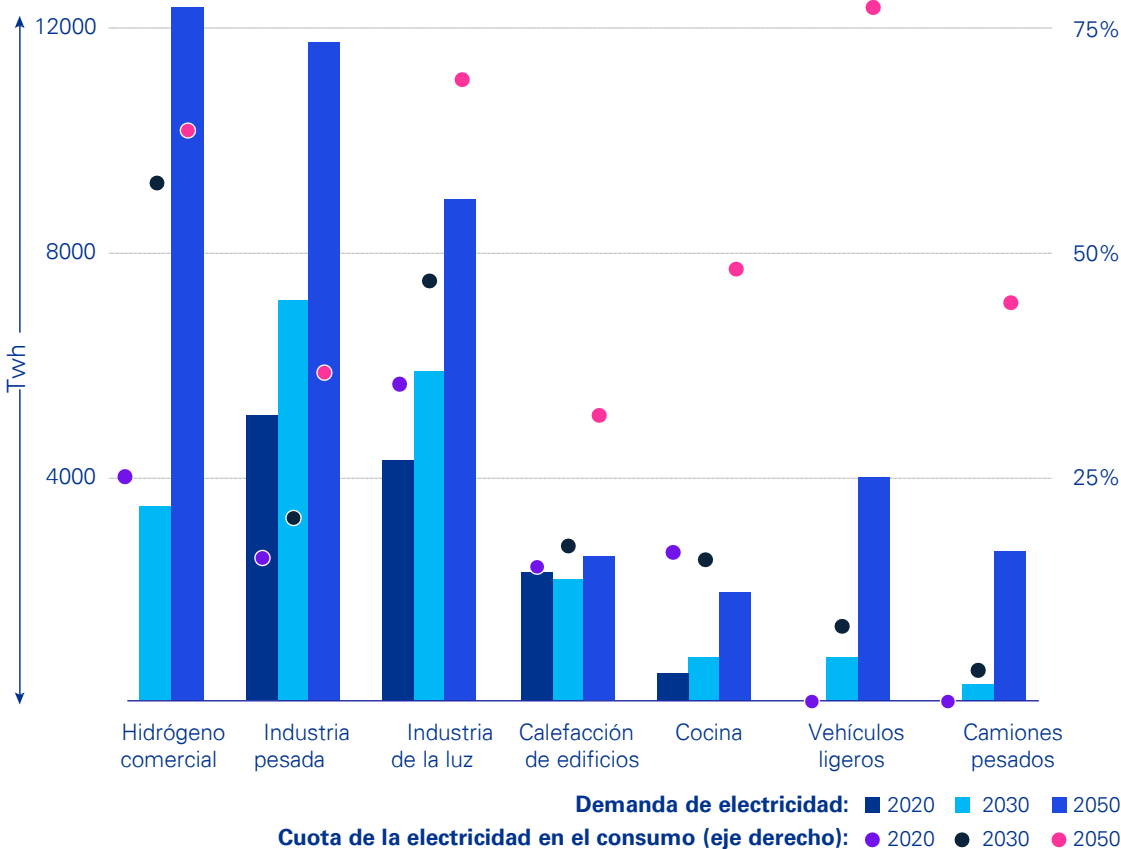
Riesgo de distribución: satisfacer las demandas en evolución de los clientes

La topología de la generación de energía está cambiando con la transición a una red más distribuida y descentralizada, con muchos actores nuevos, a menudo capaces de generar su propia electricidad (renovable) y vendérsela a otros. Todo ello transfiere el poder a los consumidores y amenaza los flujos de ingresos de energía y servicios públicos, ya que a los clientes les resulta más fácil cambiar de proveedor o incluso producir energía ellos mismos, con la ayuda de una rápida digitalización. La gestión de la red es cada vez más compleja, y las compañías de energía y servicios públicos deben asegurarse de equilibrar los suministros de energía de los numerosos proveedores para no sufrir daños en su reputación.



Acción: Es vital incorporar la resiliencia en la red mediante una planificación de escenarios más eficaz para predecir la demanda y planificar en consecuencia para evitar cortes de suministro. Las compañías de energía y servicios públicos deben trabajar en estrecha colaboración con otras partes interesadas de la red y crear redundancia en el sistema para que una falla no haga caer toda la red.

Demanda mundial de electricidad y cuota de la electricidad en el consumo de energía⁶



Notas: Hidrógeno comercial = hidrógeno producido por una empresa para venderlo a otras. Vehículos ligeros = turismos y furgonetas. Camiones pesados = camiones de carga media y camiones de carga pesada.

⁶ IEA, Net Zero by 2050: A Roadmap for the Global Energy Sector, mayo de 2021

Riesgos de cambio climático: mantenimiento de activos

Los incendios forestales, en particular, representan un riesgo importante para los proveedores de energía y servicios públicos. Con miles de kilómetros de gasoductos y líneas de energía eléctrica, una falla pequeña en los equipos puede provocar rápidamente un nuevo incendio. Las compañías pueden sufrir fuertes multas, y condenas por homicidio involuntario, si se descubre que provocaron involuntariamente incendios forestales al no mantener adecuadamente la infraestructura.

El cambio climático ha dejado al descubierto de forma brutal el

envejecimiento de las infraestructuras y presiona para que se conserven y sustituyan los activos y se recorte la vegetación circundante. Los activos también son muy vulnerables a otros impactos del cambio climático, como inundaciones, los vientos y las heladas, que aumentan en frecuencia e intensidad.

La ocurrencia cada vez mayor de fenómenos meteorológicos severos genera un riesgo creciente para los seguros, lo que hace que las primas aumenten hasta un punto en el que afectan los márgenes. Razón de más para mejorar las defensas.



Acción: Entre las herramientas que ayudan a conseguir una mayor resiliencia se encuentran los modelos de riesgo para detectar la infraestructura más expuesta, las inspecciones visuales y aéreas, la gestión de la vegetación, las cámaras de monitoreo, la tecnología satelital y la separación de la red en secciones más pequeñas para minimizar los daños. Los cortes de energía proactivos son el último recurso, que cortan la electricidad cuando los vientos y las condiciones de sequedad aumentan el riesgo de incendio. Y, por supuesto, las compañías de energía y servicios públicos deben invertir en activos para asegurarse de que son lo suficientemente sólidas para hacer frente a las presiones de la actualidad.



Riesgo de costos: cómo enfrentar la volatilidad

Los precios del petróleo y el gas, que ya eran altos desde la recuperación de COVID-19, se dispararon desde que comenzó el conflicto en Ucrania. Los gobiernos pueden verse presionados a subvencionar la energía por temor a que la inflación provoque disturbios civiles. El costo de la generación de energía aumentó en línea con los costos de las materias primas, el petróleo y el gas. Algunos de estos aumentos pueden transferirse a las empresas y los consumidores en un sector regulado, pero a menudo existe un tope, que inevitablemente afecta la rentabilidad.

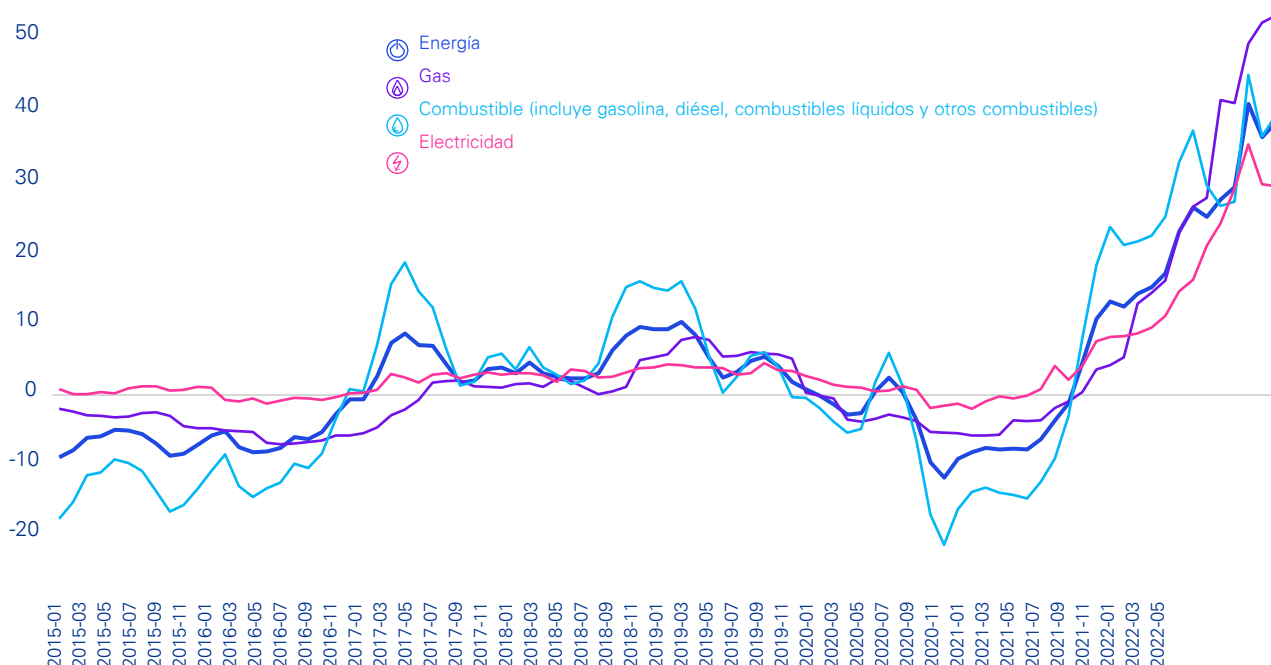
Hacer frente a esta volatilidad es un desafío, y la búsqueda de alternativas como el GNL o el cambio a las energías renovables no puede producirse de la noche a la mañana.

Los proveedores de energía y servicios públicos evaluarán cómo pueden mejorar la eficiencia operativa y la productividad para evitar tener que transferir a los clientes una parte considerable de los costos de los insumos más caros.



Acción: Los gobiernos, los reguladores y los proveedores pueden fomentar una eficiencia energética más significativa trabajando con inversionistas, reguladores, compañías eléctricas y la comunidad empresarial en general para ayudar a incubar nuevas empresas y cambiar los hábitos de los consumidores y de las empresas.

Precios de la energía en la Unión Europea en los últimos cinco años⁷ (tasa de variación anual)



⁷ Eurostat, Harmonised index of consumer prices (HICP) — monthly data (annual rate of change), mayo de 2022

Hacia un futuro resiliente

La transformación energética y la seguridad energética son vistos cada vez más como objetivos complementarios. A medida que los proveedores de energía y servicios públicos planifican un futuro resiliente, deben ganar más confiabilidad sobre el suministro de combustibles fósiles tradicionales y, al mismo tiempo, asegurar la inversión en energías renovables, y posiblemente nuclear, para lograr un nivel de diversidad que los haga más autosuficientes.

La guerra en Ucrania demostró lo rápido que pueden cambiar las situaciones. Si se añaden las amenazas cibernéticas y los riesgos relacionados con el clima, hay aún más razones para establecer una sólida planificación de resiliencia y respuesta a incidentes para mantener los activos nacionales vitales en funcionamiento en un mundo volátil.

Gran parte de lo que puede suceder está fuera del control de la industria de energía y servicios públicos. Sin embargo, aquí presentamos algunos pasos para ayudar a su organización a posicionarse y prepararse lo mejor posible, independientemente de lo que ocurra en 2022 y más allá:

- 1** Prepare un plan para gestionar inversionistas activistas y otras partes interesadas que utilizan cada vez más cuestiones ESG (medioambientales, sociales y de gobernanza) para abrir la puerta.
- 2** Revise el manual de estrategias para crisis de su organización. ¿Incluye todos los escenarios posibles y se actualiza regularmente?
- 3** Revise la filosofía de gestión de riesgos de las materias primas de su organización. Prepárese para ver cómo los cambios a corto y largo plazo en el entorno de precios podrían afectar la opinión de los clientes y accionistas y la participación del gobierno.
- 4** Comprenda cómo la legislación propuesta y las acciones gubernamentales podrían afectar a su compañía: ¿su organización tiene la flexibilidad necesaria para cambiar de marcha rápidamente y aprovechar las oportunidades que se presentan cuando cambian las agendas políticas?
- 5** Centrarse en la construcción de vínculos: continúe o aumente los esfuerzos para establecer vínculos con todas las partes interesadas relevantes, incluidos los grupos de consumidores, los gobiernos, los reguladores y la sociedad. Del mismo modo, considere los esfuerzos de cooperación de la industria y entre industrias para dar forma de manera proactiva a una regulación razonable con los gobiernos.
- 6** Ponga en orden sus cadenas de suministro: revise su configuración actual y determine cómo puede reducir las interrupciones y mejorar la resiliencia.
- 7** Revise la protección de defensa cibernética de su organización: el riesgo de una brecha cibernética es quizás el riesgo más subestimado en la industria de energía y servicios públicos. Trasciende los riesgos políticos y geográficos, y cualquier empresa, independientemente de su tamaño, es un objetivo potencial. Usted es vulnerable a una violación de seguridad cibernética sin importar dónde opere.

Sobre los autores



Valérie Besson

Líder Regional de Energía y Recursos Naturales para Europa/Oriente Medio/África (EMA) y Líder Nacional de la industria, Energía y Servicios Públicos KPMG en Francia
E: valeriebesson@kpmg.fr



Anish De

Líder global de la industria, Energía y Servicios Públicos, Líder Nacional de Energía, Recursos Naturales y Químicos de KPMG en India
E: anishde@kpmg.com



Robert Johnston

Asesor especial de Energía y clima de Eurasia Group
E: johnston@eurasiagroup.net



Stefano Moritsch

Director global de geopolítica, KPMG International
E: stefano.moritsch@kpmg.co.uk

Valerie tiene 20 años de experiencia en auditoría, incluidos seis años en el extranjero, respectivamente, en las oficinas las firmas miembro de KPMG en Bucarest, Nueva York y Short Hills. Ha trabajado en varias líneas de negocios, incluidos productos industriales, mercados de consumo, energía, productos químicos y farmacéutica, e información, comunicación y entretenimiento. Ha participado en muchos compromisos además de las auditorías, como *due diligence* financiero, conversiones a IFRS y US GAAP, auditorías de *carve-out*, participación en OPI, etc. Actualmente, Valerie se especializa en clientes que cotizan en bolsa en Francia.

Anish es director global de energía y servicios públicos de KPMG y director nacional de energía, recursos naturales y productos químicos de KPMG en India. Cuenta con más de 25 años de experiencia en consultoría de la industria energético. Como reconocido experto en la industria energético, Anish ha realizado un trabajo pionero en la reforma y reestructuración de la industria, diseñado políticas sectoriales y marcos regulatorios; asesoramiento comercial y financiero; PPP; planificación estratégica, análisis económico; marcos de inversión; estrategias corporativas, planes de reestructuración, fortalecimiento institucional y desarrollo de capacidades; mercados energéticos; eficiencia energética; redes inteligentes y digitales.

Robert ("RJ") es asesor especial sobre energía y clima de Eurasia Group. RJ fundó la práctica de Energía, Clima y Recursos de la firma en 2006 y se desempeñó como CEO de la firma de 2013 a 2018, con la supervisión de un período de rápido crecimiento y expansión internacional. RJ tiene 25 años de experiencia trabajando en estrecha colaboración con clientes inversionistas corporativos e institucionales en los sectores de petróleo y gas, minería, energía eléctrica y tecnologías limpias en materia de estrategia, evaluación de riesgos, relaciones gubernamentales y comunicaciones sobre políticas, mercados y geopolítica.

Stefano dirige los esfuerzos de KPMG en todo el mundo para ayudar a las empresas y los gobiernos a enfrentar los desafíos geopolíticos actuales. Al unir los puntos entre las tendencias macropolíticas y sus implicaciones comerciales en varios sectores, Stefano ayuda a las empresas mundiales no solo a sobrevivir, sino a prosperar en la volatilidad geopolítica. Ayuda a identificar el "y ahora" de las macro tendencias por medio de la planificación de escenarios estratégicos, *due diligence* y la gestión de riesgos geopolíticos. Con una formación académica en relaciones internacionales, diplomacia y derecho internacional, Stefano está ansioso por llevar a su puesto varios años de práctica de consultoría de gestión en Australia, donde ayudó a clientes corporativos, asociaciones industriales y clientes gubernamentales a navegar por entornos regulatorios complejos en todo el mundo.

03

ESG y seguridad cibernética son dos caras de la misma moneda

En la transición a la energía verde, la moneda clave es la confianza.

Por: Prasanna Govindankutty, Ronald Heil y Kristy Hornland



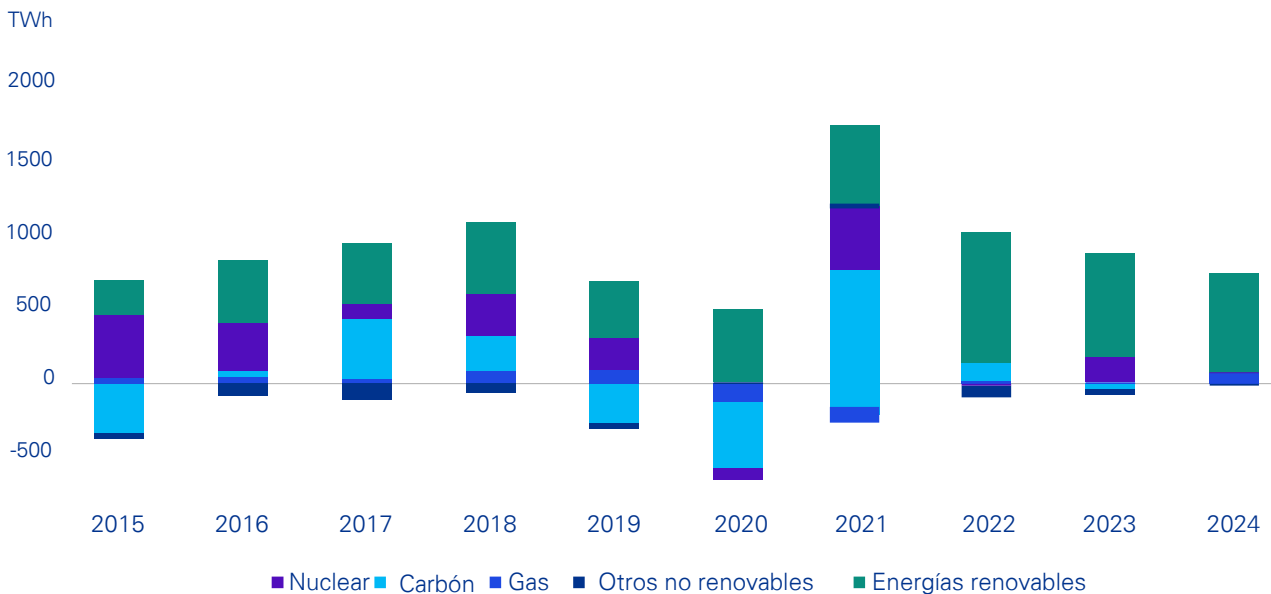
En medio de una guerra brutal en Europa del Este, se presta mucha atención a la seguridad energética. Los países con una mayor proporción de fuentes renovables pueden sentirse mejor posicionados para resistir la volatilidad de las cadenas de suministro de combustible y seguir alimentando a la industria, el comercio y los servicios públicos.

Muchos países se han comprometido a acelerar su transición a las energías renovables. Alemania, que depende en gran medida del gas ruso, anunció planes para abandonar por completo el carbón en 2030, ocho años antes de su objetivo original. Ahora tiene como objetivo obtener el 80% de su electricidad de fuentes renovables para 2030. Francia y Austria van en la misma dirección, mientras que Polonia, uno de los mayores consumidores de carbón de Europa, está realizando importantes inversiones en energía eólica¹

Estas ambiciones se alinean con los Objetivos de Desarrollo Estratégico de la ONU y tienen eco entre los ciudadanos, los gobiernos y los inversionistas. Pero, con el mundo cada vez más dependiente de la electricidad, las energías renovables deben pasar la prueba de confianza y demostrar que pueden ofrecer la confiabilidad de suministro permanente que esperan los usuarios. Si no lo hacen, podrían socavar gravemente la revolución de la descarbonización.

“Estas ambiciones se alinean con los Objetivos de Desarrollo Estratégico de la ONU y tienen eco entre los ciudadanos, los gobiernos y los inversionistas.”

Cambios mundiales en la generación de electricidad²



¹ National Geographic, How the Ukraine war is accelerating Germany's renewable energy transition, May 2022

² IEA, Global changes in electricity generation, 2015–2024, Jan 2022

La complejidad conlleva otras amenazas cibernéticas

Las energías renovables proporcionan una mayor independencia energética, ya que la energía se genera más cerca de quienes la necesitan a partir de fuentes que se encuentran dentro de las fronteras nacionales. Los microrredes llevan este concepto un paso más allá y permiten a los proveedores más pequeños y a los consumidores individuales producir, almacenar y distribuir energía limpia. Un estudio estadounidense sugiere que una red descentralizada podría aliviar la tensión en los principales generadores de energía y satisfacer el 20% de la carga máxima para 2030³. Esto incluye baterías alimentadas por energía solar, que ofrecen un respaldo altamente confiable para instalaciones comerciales y gubernamentales. Sin embargo, las redes distribuidas también son más complejas e interconectadas, con miles y posiblemente millones de nuevos proveedores de energía, incluidos los hogares, equipados con medidores inteligentes conectados a dispositivos móviles personales. A esto hay que añadir la creciente digitalización de la tecnología operativa (OT) de las centrales eléctricas, que incluye numerosos IoT para el seguimiento del desempeño y la captura de carbono. El resultado es una gama más amplia de puntos de ataque. En sistemas cada vez más interconectados, los estados-nación y los delincuentes tienen múltiples oportunidades de piratear la red primaria por medio de individuos u organizaciones que pueden tener una seguridad cibernética más débil. Los sistemas tradicionales de tecnología operativa son a veces demasiado antiguos para recibir actualizaciones de seguridad y, sin embargo, están vinculados a otras áreas de la red que se conectan a Internet y a la cadena de suministro de software más amplia.

Otra amenaza proviene de los sistemas de administración de baterías conectadas que monitorean la seguridad y la confiabilidad. Y la electricidad definida por software, que aumenta la eficiencia de la electricidad generada por cualquier fuente renovable, también contiene código vulnerable a los *hackers*.

En una encuesta reciente realizada por la empresa de gestión de riesgos DV, menos de la mitad (47%) de los profesionales de la energía creen que su seguridad de OT es tan sólida como su seguridad de TI. Seis de cada 10 indican que su organización ahora es más vulnerable que nunca a un ataque⁴.

Luego están los cargadores de automóviles para el hogar y, en última instancia, la conectividad omnipresente para los vehículos eléctricos, lo que podría paralizar el transporte y causar accidentes. Y nuestra creciente dependencia de la electricidad renovable puede poner a prueba las redes, especialmente si las baterías de almacenamiento fallan por algún motivo. Un apagón puede dejar fuera de servicio los sistemas de agua potable, las instalaciones de aguas residuales y la infraestructura de comunicaciones, lo que afectaría a todos los aspectos de la vida cotidiana. Además, el almacenamiento en batería puede considerarse un mayor riesgo de incendio.

Desde la invasión rusa de Ucrania se han producido varios ataques cibernéticos a empresas europeas de energía eólica, directamente o por medio de sus proveedores.

En un incidente, la empresa alemana Enercon sufrió la interrupción de más de 5000 turbinas eólicas tras un ataque a su proveedor de banda ancha por satélite Viasat. Según los informes, una conocida banda de *ransomware* se atribuyó la responsabilidad de al menos un ataque y dice que compartirá los *chats* internos y el código fuente con Rusia.⁵

Estas diversas y crecientes amenazas podrían frenar la adopción de las energías renovables por parte de los gobiernos y las compañías de energía y servicios públicos. Si los consumidores sienten que los proveedores de energía verde podrían sufrir más cortes, será menos probable que utilicen sus servicios. El entusiasmo por la descarbonización puede disminuir si las personas no pueden usar sus autos eléctricos, lavar su ropa o cocinar la cena.

Un estudio estadounidense sugiere que una red descentralizada podría aliviar la tensión de los principales generadores de energía y satisfacer el 20% de la carga máxima para 2030.

³ The Brattle Group, Cost-Effective Load Flexibility Can Reduce Costs by More Than \$15 Billion Annually, junio de 2019

⁴ reNEWS, Energy industry must act 'swiftly' against cyberattack, mayo de 2022

⁵ PC Magazine, Hackers Reportedly Target Wind-Energy Companies, abril de 2022

Crear y mantener la confianza en la descarbonización

Una seguridad cibernética sólida y la presentación de informes garantizan a las partes interesadas que las compañías de energía y servicios públicos tienen operaciones seguras y resilientes que previenen y se recuperan de los ataques cibernéticos y físicos, y de las amenazas climáticas como los incendios forestales, las inundaciones, los vientos y las temperaturas extremas de calor y frío.

Dado el creciente riesgo cibernético de Rusia y otros estados-nación y grupos criminales, una cultura y un protocolo de seguridad cibernética sólidos pueden mejorar las defensas y la capacidad de respuesta. La prioridad es proteger los activos críticos que determinan si los clientes reciben energía, agua u otros servicios vitales.

Las reglas y procesos estrictos de seguridad de datos pueden hacer que los empleados sean conscientes de la seguridad cibernética y evitar las violaciones. Los activos renovables se clasifican cada vez más como infraestructura crítica, lo que obliga a los operadores a cumplir con el creciente volumen de regulaciones de seguridad cibernética. Las multas reglamentarias pueden ser una desagradable llamada de atención y dañar la confianza, pero una organización con conciencia cibernética no debe actuar principalmente por miedo, sino por el deseo de hacer lo correcto y mantener el servicio al cliente.

Todas las compañías de energía y servicios públicos necesitan un marco estándar para medir el riesgo cibernético y procedimientos transparentes para restaurar el servicio tras un ataque. En toda la red, los sensores de IoT y otras herramientas de recopilación de datos pueden ayudar a detectar posibles problemas derivados de agresiones cibernéticas y físicas (así como tormentas, incendios y otros fenómenos naturales).

Existe una falta de consistencia mundial en los estándares y prácticas de seguridad cibernética y una necesidad urgente de converger y compartir información para hacer que toda la industria de las energías renovables sea más resiliente, lo que puede ayudar a garantizar la confianza y, con suerte, acelerar su adopción. Dado el papel único de la infraestructura de energía y servicios públicos en la existencia de una nación y la naturaleza interconectada de la energía, es probable que los gobiernos se involucren más y colaboren con los actores privados en toda la cadena de suministro.

A medida que los proveedores de energía y servicios públicos se vuelven más digitales, sus estrategias de ESG y cibernéticas deben alinearse con los datos en el centro. Los datos impulsan todas las decisiones en materia de ESG, ya sea la evaluación de la sostenibilidad de los proveedores, el seguimiento de la huella de carbono, la medición de la diversidad de la mano de obra, la detección de fugas de datos y, lo que es más importante, la presentación de informes sobre los avances en materia de ESG para satisfacer la creciente demanda de transparencia.

Los directores deben mantenerse al tanto de la evolución de las normas de presentación de informes de la industria y asegurarse de que sus organizaciones proporcionen la información y los conocimientos necesarios. Presentar políticas corporativas sólidas de cibernética, cumplimiento y riesgo es vital para ganar la confianza y gestionar la transición a ESG. Del mismo modo, la percepción de un desempeño bajo de los activos renovables puede dañar la confianza en ESG y frenar las agendas sostenibles de los gobiernos.

Las cuestiones de ESG pueden traer beneficios al sector de energía y servicios públicos, así como riesgos considerables. Al comprometerse plenamente con el espíritu de los negocios sostenibles y con propósito y construir una gobernanza sólida, las compañías de energía y servicios públicos pueden desempeñar un papel esencial para ayudar a las sociedades a ser más ecológicas, seguras y resilientes.

“Las reglas y procesos estrictos de seguridad de datos pueden hacer que los empleados sean conscientes de la seguridad cibernética y evitar violaciones. Los activos renovables se clasifican cada vez más como infraestructura crítica, lo que obliga a los operadores a cumplir con el creciente volumen de regulaciones de seguridad cibernética.”



Elementos críticos de un sistema de energía renovable resiliente

Gobernanza

Nombrar a un alto ejecutivo responsable de los riesgos de seguridad cibernética y ponerse de acuerdo en la frecuencia de los informes de riesgo cibernético.

Activos

Estar al tanto de todos los activos que pueden necesitar protección cibernética.

Vulnerabilidades

Comprender las vulnerabilidades y actualizar los conocimientos a medida que evolucionan las amenazas.

Monitoreo

Monitorear continuamente los sistemas y activos.

Cumplimiento de seguridad

Estar al tanto de la evolución de las normas y regulaciones de la industria para la práctica y la divulgación.

Cultura

Asegurar que todos los empleados reciban una capacitación integral en seguridad cibernética, y que los profesionales senior de seguridad cibernética participen en foros de intercambio de conocimientos de la industria.

Informes

Realizar un seguimiento e informe sobre la eficacia de las defensas de seguridad cibernética y el origen, el volumen y la gravedad de los incidentes.

Cómo puede ayudar KPMG

Adoptar una metodología práctica para sus informes de seguridad cibernética puede promover la confianza digital en su organización. Las firmas de KPMG pueden ayudar a prestar una serie de servicios y cambiar las metodologías para permitir que su organización construya confianza digital, que incluye:

- Evaluaciones de madurez cibernética (CMA) para examinar la postura de su panorama actual de amenazas y riesgos, así como el cumplimiento de las regulaciones actuales de la industria
- Desarrollo del modelo operativo objetivo (TOM) y de la gestión del cambio para gobernar su programa cibernético
- Asociación con las principales plataformas de descubrimiento de IoT/OT para ayudarlo a descubrir sus activos operativos y mantener su visibilidad
- Soporte de servicios gestionados para monitorear alertas IDS/IPS de tecnología operativa
- Programas de gestión de vulnerabilidades para garantizar que sus sistemas permanezcan operativos y protegidos
- Programas de capacitación y concientización cibernética diseñados para entornos y personal de OT
- Análisis de datos avanzados para evaluar la situación actual de su programa de seguridad



Sobre los autores



Prasanna Govindankutty

Director, Asesoramiento, Servicios de Ciberseguridad de KPMG en EE. UU.

E: pkgovindankutty@kpmg.com

Prasanna lidera los servicios de gobierno, riesgo y cumplimiento (GRC) cibernético de KPMG en EE. UU. En este puesto, es responsable de la dirección estratégica de la oferta de servicios, incluido el desarrollo de capacidades, las asociaciones con proveedores y la creación de equipos. Con dos décadas de experiencia en consultoría y en la industria, Prasanna ayuda a los clientes a transformar de manera integral sus funciones de gestión de riesgos cibernéticos y tecnológicos por medio de estrategias personalizadas y tecnologías líderes en el mercado.

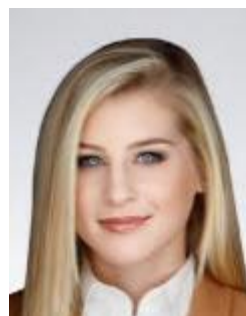


Ronald Heil

Líder mundial de seguridad cibernética de Energía y recursos naturales de KPMG International y socio de KPMG en los Países Bajos

E: heil.ronald@kpmg.nl

Ronald es socio de KPMG en los Países Bajos y líder global de cibernética de la industria de Energía y recursos naturales de KPMG International. Tiene una amplia experiencia ayudando a empresas internacionales a conectar sus productos y dispositivos al Internet de las Cosas y proporcionando asesoramiento sobre seguridad de la información y ICS/SCADA.



Kristy Hornland

Gerente, Servicios de seguridad cibernética de KPMG en EE. UU.

E: khornland@kpmg.com

Kristy es gerente dentro de la práctica de Defensa de seguridad cibernética de EE. UU. y ha pasado los últimos ocho años trabajando con clientes de servicios públicos para transformar su situación de seguridad mediante el diseño, implementación, y la puesta en marcha de programas de protección de datos cibernéticos en entornos mixtos *prem* y en la nube. Ha implementado programas de protección de datos (tecnologías y procesos) de empresas de servicios públicos internacionales y nacionales, lo que permite a los clientes mejorar su situación de seguridad y aprovechar la cibernética como un habilitador comercial en lugar de una barrera. Kristy ha desarrollado un liderazgo intelectual en el espacio IoT/OT en torno a las tecnologías conectadas emergentes y el riesgo cibernético que las acompaña y es presentadora del podcast Perspectives in IoT de KPMG.

04

De la continuidad a la resiliencia

Nuestra creciente dependencia de la electricidad hace que sea más crítico que nunca construir una organización proactiva y resiliente para garantizar la continuidad del servicio.

Por: Ali Abedi, Cassandra Hogan, Onur Karakus y Ramsay Sawaya



“Demasiado grande para fallar” es una frase usada en exceso, pero es relevante y apropiada en el caso de la energía y los servicios públicos.

La electricidad sustenta prácticamente todos los aspectos de nuestras vidas. Sin embargo, la generación y el suministro de energía se encuentran bajo la creciente amenaza de los desastres naturales, los ataques cibernéticos, el envejecimiento de la infraestructura y la fuerza laboral y las interrupciones de la cadena de suministro. Al mismo tiempo, la industria está empezando a entender los sistemas de red complejos y descentralizados, las fuentes de energía renovable y la digitalización.

Las empresas eléctricas y los servicios, tanto públicos como privados, siempre se centraron en mantener las luces encendidas y el agua fluyendo, pero la naturaleza cambiante de los riesgos desplazó el énfasis de la respuesta y la recuperación a la resiliencia por diseño para mantener los servicios las 24 horas del día, los 7 días de la semana.

Los reguladores esperan que los estándares de resiliencia operativa, comercial y financiera sean más altos en toda la cadena de suministro. La Directiva NIS 2 propuesta por la Unión Europea podría obligar a las compañías de energía y servicios públicos (y otros sectores) a demostrar nuevos niveles de seguridad cibernética¹. Si no se toman las medidas preventivas adecuadas, es posible que las empresas, y sus líderes, se vean expuestas a multas y penas privativas de libertad.

En este artículo, analizamos más a fondo los principales impulsores de la resiliencia y analizamos cómo las compañías de energía y servicios públicos pueden integrar estos elementos para mantener sus servicios.

“
La Directiva NIS 2
propuesta por la Unión
Europea podría obligar
a las compañías de
energía y servicios
públicos a demostrar
nuevos niveles de
seguridad cibernética.”



¹ European Commission, Commission welcomes political agreement on new rules on cybersecurity of network and information systems, mayo de 2022

Amenazas naturales

El cambio climático es una gran y creciente preocupación para la industria. Las tormentas, los incendios forestales y de matorrales, las inundaciones, los vientos, el calor y el frío extremos y las sequías dejaron de ser fenómenos extraños para convertirse en fenómenos naturales frecuentes en muchos lugares. Estados Unidos ha sufrido 323 catástrofes meteorológicas y climáticas desde 1980, con daños estimados en US\$ 2195 billones². Y entre 2013 y 2020, la cantidad de horas de apagón por año se duplicó de cuatro a ocho.³

En India, en 2022, más de 1000 millones de ciudadanos han estado luchando para hacer frente a temperaturas insostenibles muy por encima de los 40 °C, la primavera más calurosa en la historia del país, lo que impidió el trabajo al aire libre y provocó cortes de energía, escasez de agua, racionamiento impuesto por el Estado, cancelaciones de trenes, así como la reducción de la producción industrial y agrícola⁴.

Además de dañar la infraestructura física, estos fenómenos también pueden retrasar las cadenas de suministro de piezas y materiales vitales. Y las compañías de energía y servicios públicos no solo tienen que hacer frente a los efectos del cambio climático en sus operaciones; también deben considerar el impacto de su propia organización en el medioambiente y la sociedad, ya sea respecto a las emisiones de carbono o el trato a los trabajadores.



² National Centers for Environmental Information, Billion-Dollar Weather and Climate Disasters, Accessed 10 June 2022

³ US Energy Information Administration, US electricity customers experienced eight hours of power interruptions in 2020, noviembre de 2021

⁴ Bloomberg, Climate Change Turned Up India's Heat. But by How Much?, mayo de 2022

Amenazas operativas



Descentralización y digitalización

Las redes están cada vez más distribuidas, con franjas de fuentes más pequeñas y localizadas, que crean una mezcla híbrida de energía convencional/nuclear y, cada vez más, de energía renovable procedente de pequeñas centrales hidroeléctricas, biomasa, biogás, energía solar, eólica y geotérmica.⁵ Es un gran dolor de cabeza orquestar este complejo entramado de actores para mantener la integridad del sistema.

Al mismo tiempo, la digitalización aporta una mayor automatización y sofisticación a los sistemas de control, integra operaciones y TI, con una creciente dependencia de una red externa en la nube y proveedores de servicios. Con una red troncal tan interconectada, una sola falla puede tener múltiples consecuencias y potencialmente cerrar toda la instalación.

Cualquier incidente expone instantáneamente las muchas interdependencias de la sociedad, en la que un corte tiene una reacción en cadena que afecta las telecomunicaciones, la industria, el transporte y el agua. Por ejemplo: si no hay una red móvil o Internet, es más difícil contactar a los ingenieros y al resto del personal de reparación. Y si no hay energía eléctrica y las gasolineras no funcionan, estas mismas personas no pueden conducir para llegar a los puntos de los daños. Hacer frente a las subidas de tensión es un desafío adicional cuando muchos actores están involucrados en la red, ya que los proveedores orientados al cliente buscan distribuir la energía desde múltiples ubicaciones.

A medida que los proveedores de energía y servicios públicos hacen la transición a empresas digitales, donde todos los equipos, incluido el hardware, los sensores de IoT y los dispositivos personales, están conectados, y donde muchos

⁵ Power Grid International, A look towards the future: Integrating DERMS and ADM, May 2019

terceros intervienen en la transmisión y la facturación, la amenaza, y el impacto posterior, del ataque cibernético aumentó drásticamente. Desde la pandemia, la aceleración del trabajo híbrido ha aumentado la conciencia de cómo los atacantes pueden *hackear* los sistemas en redes inseguras. El deterioro de las relaciones con otros países añade otra capa de amenaza.

Las organizaciones de energía y servicios públicos a menudo han sido blanco de delincuentes cibernéticos y de los estados nación (a veces, ambos trabajando en conjunto) para interrumpir la infraestructura nacional crítica de los enemigos. Se cree que el arma cibernética Stuxnet fue desarrollada conjuntamente por Israel y EE. UU. para atacar las instalaciones nucleares iraníes, aunque tanto Israel como Irán lo niegan⁶. Stuxnet eliminó los sistemas SCADA dentro de las instalaciones nucleares iraníes críticas.⁷

Otro ejemplo es NotPetya, que, según los expertos, tiene como objetivo Ucrania⁸. McAfee afirma que "... esta variante fue diseñada para propagarse rápidamente", y que tiene como objetivo "empresas de energía completas, la red eléctrica, estaciones de autobuses, estaciones de servicio, aeropuertos y bancos".

Es posible que las organizaciones no sean un objetivo directo, pero terminen con daños colaterales, ya que el *malware* lanzado 'a la naturaleza' explota sus vulnerabilidades. Es posible que Stuxnet haya tenido un objetivo específico, pero el código utilizado para desarrollar el *malware* original se ha mejorado y puede utilizarse para atacar a un público mucho más amplio en todos los sectores y zonas geográficas.

Puede que NotPetya haya tenido en el punto de mira al sector energético, y posiblemente a Ucrania. Aun así, ha impactado a muchas organizaciones globales, incluido el avión Antonov en Ucrania, el gigante logístico Maersk y el productor de petróleo ruso Rosneft.⁹

No es raro que los *hackers* hostiles sigan un ataque cibernético con un ataque físico. El área de ataque es amplia debido a las enormes redes de estaciones, torres de alta tensión y otras instalaciones. La falta de una fuente de energía de reserva hace que sea aún más difícil recuperarse mediante la puesta en marcha de un generador.

Envejecimiento de los activos y de la mano de obra

En un sector con muchos activos, la sustitución y el mantenimiento rentables son factores constantes. El cambio climático ha recordado a las compañías de energía y servicios públicos la facilidad con la que algunos equipos pueden dañarse. En el caso de los incendios forestales, en particular, la caída de torres y líneas eléctricas puede ser responsable de la pérdida de vidas y medios de subsistencia, lo que da lugar a cuantiosas multas o incluso a acciones penales contra los ejecutivos por no adoptar las medidas preventivas adecuadas.

Sin el personal y las habilidades adecuadas, las redes de energía y servicios públicos pueden tener dificultades para alcanzar los niveles de continuidad que exigen los clientes. A medida que la generación de trabajadores de más edad se acerca a la jubilación, es vital atraer nuevos talentos al sector y transmitir las décadas de experiencia de las generaciones anteriores. Y a medida que los roles se vuelven cada vez más digitales, las capacidades tecnológicas, en combinación con la automatización, se vuelven esenciales.

“Es posible que Stuxnet haya tenido un objetivo específico, pero el código utilizado para desarrollar el *malware* original se ha mejorado y puede utilizarse para atacar a un público mucho más amplio en todos los sectores y zonas geográficas.”

⁶ The New Yorker, World War Three, By Mistake, diciembre de 2016

⁷ Foreign Policy, Stuxnet's Secret Twin, noviembre de 2013

⁸ Wired, What is the Petya ransomware spreading across Europe? WIRED explains, julio de 2017

⁹ BBC, Global ransomware attack causes turmoil, junio de 2017

Creación de un marco y una cultura de resiliencia

A medida que se esfuerzan por construir organizaciones seguras y sólidas que puedan proporcionar servicios ininterrumpidos a las organizaciones públicas y privadas y a los ciudadanos, las compañías de energía y servicios públicos están tratando la resiliencia como un imperativo a nivel de directorio.

Reino Unido cuenta con una Estrategia Nacional de Resiliencia¹⁰ diseñada para hacer frente a condiciones meteorológicas extremas, terrorismo, pandemias, ataques cibernéticos, inestabilidad geopolítica y accidentes.

La Red Nacional del país adopta una metodología de "Sistemas Integrales"¹¹. Y en EE. UU., el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) proporciona una base técnica para mejorar el diseño, la construcción, la operación y el mantenimiento de los edificios y los sistemas de infraestructura¹²

Marco integrado de resiliencia

Definir el alcance y comprender las necesidades y los requisitos de las partes interesadas

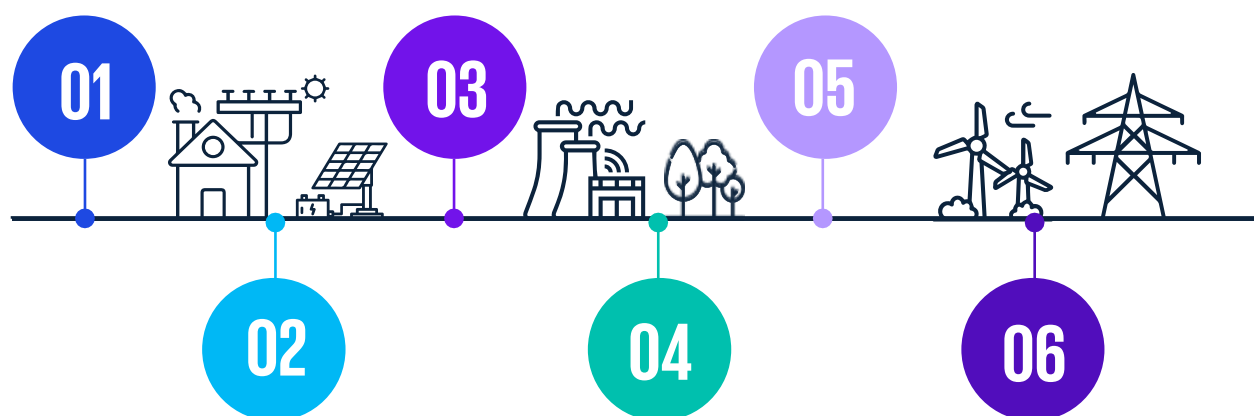
- Considerar la amenaza y los subsistemas de interés
- Definir las expectativas de las partes interesadas

Desarrollar y evaluar las mitigaciones de resiliencia

- Desarrollar mitigaciones y alternativas de resiliencia
- Evaluar el impacto en el riesgo de resiliencia
- 4 R: Redundancia, resistencia, respuesta y recuperación

Implementar y medir

- Desarrollar informes posteriores a la acción y de lecciones aprendidas
- Métricas y KPI



Evaluación de riesgos para determinar las susceptibilidades y vulnerabilidades de las amenazas

Desarrollar un plan de resiliencia



Objetivo del sistema

Mantener la disponibilidad de energía para el cliente y los consumidores

¹⁰ UK Government, National Resilience Strategy: Call for Evidence, julio de 2021

¹¹ National Grid, Our Whole System approach, marzo de 2021

¹² National Institute of Standards and Technology, Resilience, acceso en junio de 2022

Una estrategia de resiliencia debe presentar las siguientes características:

Modelización de fenómenos meteorológicos extremos

Los planificadores de energía y servicios públicos deben mejorar su planificación de escenarios para hacer frente a las amenazas del cambio climático. Los eventos históricos ya no son un predictor confiable del futuro, por lo que los modelos deben incorporar más datos en tiempo real y utilizar innovaciones como gemelos digitales para prever la probabilidad y la gravedad del impacto en la infraestructura y los servicios interdependientes.

Preparación de equipos y personas

La preparación es igualmente fundamental: invertir en una infraestructura más nueva y sólida, almacenar inventario y tener personal adicional y contratistas disponibles para hacer las reparaciones lo más rápido posible. Es posible que los profesionales de adquisiciones tengan que reconsiderar sus ambiciones “justo a tiempo”, dado el enorme costo potencial y los inconvenientes de una interrupción. Esto implica decisiones de costo-beneficio: si se prepara en exceso, los gastos aumentarán considerablemente; si no se prepara adecuadamente, corre el riesgo de que se produzcan cortes inaceptables, clientes insatisfechos y enormes facturas por reparaciones. Además, algunos tipos de inventarios, como los super transformadores de red, son tan específicos para las distintas partes de la red que es imposible tener todos los artículos en stock.

Endurecimiento

Las compañías de energía y servicios públicos pueden tomar muchas medidas para hacer más resiliente su infraestructura física,

como instalar postes más resistentes, soterrar las líneas aéreas, podar los árboles y elevar las subestaciones por encima de los niveles de inundación previstos.

La planificación de escenarios a más largo plazo puede guiar la reflexión para considerar las condiciones climáticas probables en las próximas décadas.

Las inversiones en reemplazo y mantenimiento deben equilibrar los costos iniciales ahora y los gastos potencialmente significativos más adelante para remediar los daños. Los estudios tienden a mostrar que las actualizaciones son muchas veces más baratas que las reparaciones: un estudio realizado en EE. UU. concluyó que cada dólar invertido en la mitigación de desastres o “reforzamiento” evitaba seis dólares en costos de reconstrucción¹³. En un caso, mediante la instalación de nuevos monitores de transformadores, una empresa evitó un apagón a 15.000 clientes, lo que ahorró aproximadamente US\$ 1 millón en gastos de restauración¹⁴.

Cada vez hay más interés en el mantenimiento predictivo, con el uso de sofisticados sensores, drones y otros IoT, que, combinados con análisis avanzados, pueden ayudar a determinar cuándo pueden fallar los equipos, iniciando una acción proactiva. Las plataformas predictivas basadas en la nube utilizan la IA y la automatización para mejorar constantemente su capacidad de detectar defectos en los activos y, así, evitar el tiempo de inactividad de los equipos. Y si se combinan con pronósticos meteorológicos extremos precisos, las empresas pueden estar mejor preparadas.

Una forma de crear resiliencia es mediante la redundancia, de

modo que las diferentes líneas de transmisión puedan operar de forma independiente entre sí; si una falla, las otras siguen trabajando.

El monitoreo es esencial para este abordaje, ya que detecta cualquier problema operativo, como ataques cibernéticos o fallas mecánicas, y permite que los sistemas los aislen para “fallar de manera segura” y evitar una interrupción más amplia del sistema.

La generación distribuida incorpora más fuentes alternativas a la red, incluido el uso cada vez mayor de microrredes. El almacenamiento de energía puede aumentar la resiliencia, ya que proporciona una fuente de energía alternativa que actúa como carga y generador.

Seguridad cibernética

Y, por supuesto, la defensa cibernética se está convirtiendo en una gran prioridad, con la necesidad urgente de establecer culturas de conciencia cibernética y estrictos protocolos de entrada. También es vital identificar y anular las posibles amenazas y restaurar los sistemas en el caso de que sufran un ataque. Algunos están eliminando la tecnología heredada antigua y pasándose a la nube para eliminar la mayor cantidad posible de posibles vulnerabilidades.

Creación de una cultura de resiliencia

Por último, incorporar conocimiento al sistema puede ayudar a evitar el riesgo de la “persona clave”, cuando las organizaciones dependen de las habilidades únicas de los individuos. La planificación estratégica de la mano de obra identifica las habilidades y los líderes necesarios y el entorno de trabajo que atraerá a una fuerza laboral nueva y diversa. Invertir en la capacitación de habilidades técnicas y crear nuevas vías de reclutamiento y de contratistas/independientes probablemente sea crucial.

¹³ Federal Insurance and Mitigation Administration, Natural Hazard Mitigation Saves Interim Report, junio de 2018

¹⁴ T&D World, Ushering in the Next Era of Grid Modernization, diciembre de 2021

Inversión en un futuro confiable y seguro

La resiliencia no solo mantiene las luces encendidas; genera confianza e impulsa la ventaja competitiva.

En una organización centrada en la resiliencia, la dirección es claramente responsable de proteger la prestación de servicios, con el apoyo de datos sólidos que pueden aportar información para la inversión en resiliencia a más largo plazo, cumplir con los requisitos reglamentarios en evolución y ayudar a garantizar una acción preventiva rápida en el caso de fallas. La planificación de la resiliencia tiene tres áreas principales:



Preparar

- Gestión de servicios empresariales
- Marcos de control de la resiliencia
- Gestión de escenarios y tolerancia



Evaluar

- Evaluación de la resiliencia de los servicios no estresados
- Evaluación de la gestión de las amenazas del servicio
- Evaluación de la resiliencia de los servicios sometidos a estrés



Acción

- Elaboración de informes, soluciones y evaluación de la inversión
- Mejora del servicio
- Planificación y gestión de la recuperación

Cómo KPMG puede ayudar

Los profesionales de energía y servicios públicos de KPMG tienen una amplia experiencia en la creación de organizaciones más sólidas y pueden ayudarlo a:

- Hacer que la resiliencia y la confianza sean los cimientos de su estrategia organizacional y su propuesta de valor
- Ser ágil y flexible para mantener los resultados comerciales después de eventos disruptivos
- Mantener su empresa conectada interna y externamente, antes y después de la interrupción
- Hacer que su resiliencia esté basada en datos y tecnología para generar información oportuna, reducir costos y mejorar la escalabilidad

Esto debería proporcionarle una visibilidad y un control claros de los servicios, los recursos y los riesgos, lo que permitiría garantizar la estabilidad de los servicios en tiempos de interrupción. También puede apoyar al negocio, a los clientes y a los mercados financieros para que la resiliencia se convierta en una ventaja competitiva crítica y en un motor de confianza.



Sobre los autores



Ali Abedi

Director senior,
Resiliencia cibernética
— Global Cyber SGI de
KPMG en Reino Unido
E: ali.abedi@kpmg.co.uk

Ali lidera la capacidad de Resiliencia cibernética en KPMG de Reino Unido. Con más de 25 años de experiencia en el diseño, desarrollo e implementación de soluciones de resiliencia en múltiples sectores industriales, incluidos los de energía y servicios públicos, Ali ha creado soluciones de resiliencia cibernética para organizaciones influyentes con una amplia huella mundial, lo que garantiza que las soluciones cubran el impacto de las amenazas cibernéticas por país y región en todo el mundo. Estas soluciones se desarrollaron para las capacidades de respuesta operativas, tácticas y estratégicas de las principales organizaciones, lo que garantiza que toda la organización pueda responder adecuadamente a los principales eventos cibernéticos.



Cassandra Hogan

Líder nacional de la
industria, energía y
recursos naturales de
KPMG Australia
E: cjhogan@kpmg.com.au

La pasión de Cassandra por la industria energético comenzó al inicio de su carrera, en su primer trabajo en un gran centro de llamadas de servicios públicos. Esto le dio a Cassandra una enorme apreciación de la orientación al cliente y la basó en la importancia de “ponerse manos a la obra y cumplir los compromisos”. Lo que siguió fueron 16 años en una amplia gama de funciones, desde operaciones de primera línea, estrategia, integración de fusiones y transformación de negocios en un período de cambios significativos en la industria energético.

Como líder nacional de la industria de energía y recursos naturales, Cassandra aporta una perspectiva completa y firme sobre los problemas, consciente de que las soluciones técnicas son tan buenas como su capacidad de implementación. Cassandra también es mentora de mujeres en la industria de energía y recursos naturales.



Onur Karakus

Consultor senior,
estrategia y riesgo
cibernético
KPMG en los Países Bajos
E: karakus.onur@kpmg.nl

Onur es un especialista en gestión de riesgos de resiliencia empresarial que tiene más de 10 años de experiencia en este campo. A lo largo de su carrera, ha dirigido y entregado múltiples proyectos de continuidad comercial relacionados con los riesgos cibernéticos y de interrupción del negocio. Onur ha acumulado una amplia experiencia en resiliencia empresarial, particularmente en la industria energético, y ha ayudado a los líderes de la industria a formular e implementar estrategias de continuidad empresarial. Ayuda a las organizaciones a percibir los entornos de riesgo disruptivos, a gestionar los riesgos y a preparar las mejores estrategias de respuesta posibles con la ayuda de la tecnología y la seguridad cibernética.



Ramsay Sawaya

Director General, Estrategia de
Energía y Servicios Públicos
KPMG en los EE. UU.
E: ramsaysawaya@kpmg.com

Ramsay tiene 30 años de servicio en servicios públicos de electricidad y gas. Su experiencia consiste en liderar la transformación de las empresas de servicios públicos en materia de ESG, riesgo y resiliencia, y la gestión de activos e inversiones para ayudar a las compañías de servicios públicos de electricidad y gas a navegar en un entorno empresarial cambiante. Ha apoyado el desarrollo de la dirección estratégica y ha evaluado e implementado prácticas líderes en gestión de riesgos, resiliencia y activos en toda la industria.

05

Preparación para incidentes: un manual de estrategias para su peor día

Estar preparado para un incidente cibernético puede minimizar la interrupción de la infraestructura crítica de energía y servicios públicos.

Por: Jason Haward-Grau, Lars Jacobs y Maliha Rashid



En los últimos años, las amenazas cibernéticas para las organizaciones de energía y servicios públicos han aumentado significativamente, en particular debido a los ataques cada vez más sofisticados de *ransomware* y *malware*. El *malware*, en particular, puede propagarse rápidamente e interrumpir procesos, robar datos, amenazar la seguridad y cortar los servicios vitales para el gobierno, las empresas y los consumidores.

Más de un tercio (37%) de las organizaciones han sido atacadas por ransomware solo en el último año¹, y una cuarta parte (26%) se ha visto obligada a cerrar algunas operaciones². Los incidentes también tienen consecuencias más graves, ya que el tiempo de inactividad promedio aumentó de 5 a 26 días³ en los últimos años y los pagos promedio de ransomware aumentaron en 144% desde 2020⁴

La industria de energía y servicios públicos enfrenta un riesgo constante y creciente, desde un intento de envenenamiento en una ciudad de Florida en 2021, por medio del *hackeo* al sistema de tratamiento de agua⁵, hasta un ataque cibernético presuntamente patrocinado por el estado a las redes eléctricas de India en 2022, por medio de cámaras y dispositivos IoT⁶

El estado de la tecnología operativa (OT) es especialmente vulnerable, con nueve de cada diez organizaciones que experimentaron al menos una intrusión en sus sistemas en el último año⁷. Una proporción similar admite que tiene una visibilidad limitada o nula de sus entornos de sistemas de control industrial (ICS) debido a su antigüedad y a la tecnología heredada⁸

Desde la invasión de Ucrania, los *hackers* rusos han estado rondando la infraestructura energética vital de EE. UU. y otras naciones, en busca de oportunidades y puntos débiles en los sistemas digitales para robar información confidencial o interrumpir las operaciones.⁹

A diferencia de la TI, que suele tener un ciclo de vida de 3 a 5 años, muchas propiedades de tecnología operativa de energía y servicios públicos se ejecutan en software y hardware antiguos y, a menudo, sin soporte. Con la transformación digital que hace que la tecnología operativa dependa cada vez más de las TI, existe un área de ataque cada vez mayor que los *hackers* pueden y intentarán explotar. Además de los actores tradicionales, la amenaza se extiende a una serie de nuevas empresas más pequeñas que venden electricidad y gas y suministran sus medidores. Muchas de estas empresas son esencialmente operadores de marketing y servicio al cliente con seguridad cibernética relativamente inmadura.

En un mundo digital, en el que todo está conectado, los cortes de la red pueden paralizar los servicios públicos, las empresas y los hogares.

Crecimiento del ransomware

90% de las organizaciones sufrió al menos una intrusión en el sistema⁷

37% de las organizaciones afirmó que fue víctima de *ransomware*¹

26% afirmó que los ataques provocaron una suspensión de las operaciones²

26 días de inactividad promedio³

US\$ 2,2 millones fue la demanda promedio de rescate⁴

¹ Sophos, The state of Ransomware 2021, Aabril de pril 2021

² Cybereason, Ransomware Attacks and the True Costs to Business, Dragos 2020 ICS Cybersecurity Year in Review

³ Coveware, Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting, mayo de 2022

⁴ Unit 42, 2022 Unit 42 Ransomware Threat Report, marzo de 2022

⁵ CNN, Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says, febrero de 2021

⁶ Business Standard, Suspected Chinese hackers collect intelligence from India's power grid, abril de 2022

⁷ Fortinet, 2020 State of Operational Technology and Cybersecurity Report, abril de 2021

⁸ Cybereason, Ransomware Attacks and the True Costs to Business, Dragos 2020 ICS Cybersecurity Year in Review

⁹ The Texas Tribute, Texas power grid, energy sectors facing elevated Russian cyber threats during war in Ukraine, marzo de 2022

No todos tienen un generador de respaldo, y un corte de energía expone instantáneamente nuestra creciente dependencia de la electricidad en todos los aspectos de la vida cotidiana. La conectividad también lleva la amenaza fuera de la organización a millones de clientes, mediante dispositivos IoT como medidores inteligentes en los hogares y acceso en línea a cuentas de facturación, lo que abre oportunidades para el *phishing* y otras formas de entrada no autorizado a los sistemas de energía y servicios públicos.

Conscientes de estos peligros, los reguladores ejercen una presión mayor sobre las empresas para que demuestren defensas cibernéticas seguras. La Ley de Ciberresiliencia de la UE busca establecer una línea de base de resiliencia en todas las industrias, con un fuerte énfasis en la infraestructura crítica de energía y servicios públicos¹⁰. En EE. UU., las Directivas de Seguridad de la Administración de Seguridad del Transporte [(TSA y publicadas a raíz de un ataque cibernético en 2021 contra Colonial Pipeline)] exigen que las empresas de electricidad y gas evalúen todos sus activos para garantizar que cumplan las normas nuevas y más estrictas y que elaboren planes claros de preparación para incidentes¹¹.

“
Además de los actores tradicionales, la amenaza se extiende a una serie de nuevas empresas más pequeñas que venden electricidad y gas y suministran sus medidores.”

Creación de una “memoria muscular” de preparación para incidentes

Una cultura de seguridad cibernética sólida puede reducir significativamente las posibilidades de un ataque, pero las organizaciones de energía y servicios públicos también deben estar preparadas en el caso de que ocurra un incidente. La preparación para los incidentes se trata de desarrollar un manual de estrategias para el “peor de los casos”, mitigar las vulnerabilidades por adelantado y documentar un plan de respuesta rápido y decisivo. Por medio de la capacitación y las simulaciones es posible desarrollar una “memoria muscular” valiosa.

La resiliencia cibernética consta de tres etapas clave: la preparación, la respuesta y la corrección. Esta última para abordar las causas de fondo y, con suerte, evitar que el problema se repita.

La preparación es la base de la resiliencia, con un plan sólido que define las funciones y responsabilidades de las diferentes partes interesadas y las acciones necesarias para responder y recuperarse rápidamente para ayudar a minimizar el impacto en la organización y sus clientes.

Los planes deben estar tanto en un formato electrónico seguro como en una copia impresa para garantizar el acceso en el caso de que los sistemas fallen. Los tres componentes de un plan de preparación son:

- **Las personas:** se establece una cadena de mando que designa a los responsables de la toma de decisiones críticas, las habilidades que deben poseer y cualquier capacitación necesaria para llenar los vacíos.
- **Los procesos:** pasos específicos de respuesta a incidentes para diferentes escenarios, comunicaciones externas e internas (incluidas las obligaciones legales) y un camino claro hacia la normalidad. Las aplicaciones de tecnología operativa de energía y servicios públicos suelen tener capacidades de copia de seguridad y recuperación menos sólidas que los sistemas de TI, por lo que es necesario fortalecerlas y otorgarles permisos de control explícitos.

- **La tecnología:** es un componente importante del plan, ya que describe los datos necesarios, los pasos y procesos para localizar y recopilar esta información, y las herramientas para analizar lo que sucedió y facilitar una recuperación rápida.

Un plan debe considerar la gama más amplia de resultados adversos, incluida la interrupción de la generación de energía o de los sistemas de extinción de incendios y otros efectos secundarios. Las ventanas de mantenimiento (tiempo necesario para solucionar los problemas) pueden verse afectadas por un ataque, por lo que es esencial realizar pruebas y controles de seguridad.

Trabajar en diferentes escenarios puede ayudar a las organizaciones a determinar el impacto de los ataques en los activos operativos vitales, como las instalaciones de almacenamiento de datos o las interfaces de administración humana, lo que podría detener la generación de energía.

Si estos activos se paralizan temporalmente, una opción es cambiar a la sala de control de la capacitación, pero esta también podría quedar fuera de servicio.

¹⁰ European Commission, Cyber resilience act — new cybersecurity rules for digital products and ancillary services, marzo de 2022

¹¹ Burns McDonnell, Cybersecurity Directives Require Quick Action by Electric/Gas Utilities, marzo de 2021

Simulación

Los simulacros o ejercicios “de mesa” son una característica habitual de la cultura de una seguridad cibernética madura, que ayuda a las organizaciones de energía y servicios públicos a mejorar su capacidad para detectar ataques de red con mayor antelación, lo que permite una contención más rápida y evitar una escalada. El simulacro debe identificar las brechas en el software de detección y en la recopilación de información, para mantenerse al tanto de las posibles amenazas en todo el mundo. Al mostrar más claramente los vínculos entre los peligros físicos y los problemas cibernéticos, permitirá una mejor apreciación del impacto más amplio de un ataque y ayudará a reducir, en primer lugar, el riesgo de que ocurra un incidente.

En un ejercicio típico, un facilitador guía al personal a lo largo de un incidente cibernético adaptado y le asigna al grupo la tarea de evaluar opciones y tomar decisiones en momentos cruciales,

con lo que expone a las personas clave a los desafíos de la vida real para volver a poner en marcha las operaciones en el menor tiempo posible. Esto mejora la preparación, hace que los participantes se familiaricen con sus responsabilidades y descubre las debilidades operativas.

Al reunir a las partes interesadas, como el CIO, el CISO, el director de operaciones de tecnología operativa o un gerente de turno de tecnología operativa, que no suelen interactuar, los simulacros de preparación para incidentes exponen a las personas a diferentes formas de ver la organización. El personal de tecnología operativa tiende a preocuparse por la seguridad operativa, la optimización de procesos y la confiabilidad, mientras que sus contrapartes de TI piensan más en la confidencialidad, la disponibilidad y la integridad.

Superar esta diferencia de mentalidad puede ayudar a los equipos a colaborar de manera más efectiva y pensar en cuestiones prácticas que quizás nunca se discutan hasta que se produzca un incidente, tales como: ¿cómo nos conectaremos todos? ¿y dónde/cómo nos encontraremos?

Una cultura de seguridad sólida y subyacente puede marcar la diferencia al difundir la conciencia cibernética y la capacidad de respuesta. Muchos proveedores de agua y energía, incluidos los solares, eólicos, de biomasa, de gas y de carbón, tradicionalmente han tenido entornos de salud y seguridad relativamente relajados, sin restricciones rígidas, salvo en el área de los generadores. Ahora que la cibernética se ha convertido en una amenaza reconocida, estas organizaciones deben crear conciencia y fomentar los buenos hábitos.



Acceso a los recursos que necesita

Los atacantes cibernéticos son cada vez más activos y los incidentes de *ransomware* y *malware* aumentan tanto en frecuencia como en gravedad. Es posible que las organizaciones de energía y servicios públicos no puedan evitar todos los ataques, pero pueden mejorar su preparación para los incidentes.

Armadas con un manual de estrategias probado y comprobado, las organizaciones de energía y servicios públicos pueden responder a tiempo, con un conjunto de tareas documentadas, una cadena de mando transparente y personas con la memoria muscular para movilizar y cerrar la amenaza lo más rápido posible, para proteger la seguridad de todos los empleados y mantener la infraestructura nacional vital en operación.

Sin embargo, un plan de preparación para incidentes es tan bueno como las personas que lo operan, por lo que las organizaciones deben centrarse en la capacitación y los recursos. Esto debería garantizar que los trabajadores pertinentes estén capacitados y entrenados en la contención y la recuperación, y que el responsable del plan sea capaz de localizar y desplegar rápidamente a las personas adecuadas. Dadas las enormes exigencias a las que se ve sometido el personal durante un incidente, en el que el equipo de TI a menudo trabaja las 24 horas, el cansancio y los errores pueden aparecer, por lo que es esencial contar con recursos de reserva para tomar el relevo.

Por último, las organizaciones de energía y servicios públicos deben reconocer que incluso el plan de preparación para incidentes más eficiente tiene un margen de mejora. Es por eso que una perspectiva externa puede ser muy valiosa para crear resiliencia. Un especialista externo cualificado puede guiar al equipo de preparación por los diversos pasos y llevar a cabo una evaluación de preparación para incidentes, además de indicar acciones recomendadas para superar las deficiencias.

Cómo podemos ayudar

En KPMG hemos llevado a cabo múltiples evaluaciones de preparación para incidentes y ejercicios de simulación para compañías de energía y servicios públicos y negocios industriales. Aportamos una amplia gama de miembros del equipo altamente cualificados y experimentados a la preparación para incidentes, desde probadores de seguridad y penetración hasta consultores operativos, expertos en preparación cibernética y profesionales de recuperación que han dirigido directamente los esfuerzos de recuperación de los clientes afectados. KPMG se complace por haber sido reconocida como "Líder" en los Servicios de Preparación para Incidentes Mundiales por IDC Marketscape in 2021.

Los clientes valoran especialmente nuestra visión multisectorial. Con demasiada frecuencia, las empresas están encapsuladas en su burbuja industrial y tienen un conocimiento limitado de las mejores prácticas en otros sectores que pueden importar y aplicar. Los profesionales de KPMG han trabajado en la preparación para incidentes y en la realización de simulacros en muchos sectores, incluidos los de servicios financieros, automotriz, químico y manufacturero.



Sobre los autores



Jason Haward-Grau

Director Gerente de Asesoría,
Servicios de Seguridad
cibernética
KPMG en los EE. UU.
E: jhawardgrau@kpmg.com

Jason Haward-Grau es un líder de la práctica de seguridad cibernética de KPMG en EE. UU., con un historial comprobado como ejecutivo cibernético en múltiples sectores y más de 20 años de experiencia en el desarrollo, entrega y mantenimiento de estrategias, programas y operaciones de seguridad cibernética en los sectores de energía, moda de lujo e infraestructuras críticas.



Lars Jacobs

Gerente Senior de Asesoría,
Servicios de Seguridad
cibernética
KPMG en los Países Bajos
E: jacobs.lars@kpmg.nl

Lars dirige la práctica de respuesta cibernética de KPMG en los Países Bajos. En ese rol, ayuda a los clientes de KPMG durante la fase de crisis de un incidente de seguridad cibernética y les aporta el conocimiento y la experiencia para prepararse de manera efectiva.



Maliha Rashid

Líder de Privacidad de
Datos, Digital e Innovación
— Cibernética
KPMG Lower Gulf
E: mrashid5@kpmg.com

Maliha es directora en la práctica de Innovación y Digital de KPMG en el Lower Gulf. Tiene más de 17 años de experiencia en seguridad cibernética y privacidad de datos en Francia y Oriente Medio. Ha dirigido programas de transformación de protección de datos y seguridad cibernética premiados en Europa y los Emiratos Árabes Unidos. Antes de unirse a KPMG, Maliha fue directora de riesgos de seguridad cibernética en una importante aerolínea. Previo a esto, trabajó con las firmas de consultoría Big Four durante más de 12 años en Francia y, más recientemente, en el Medio Oriente, donde llevó a cabo proyectos de seguridad cibernética en varios sectores, incluidos los de servicios financieros, industria, lujo y telecomunicaciones.

06

Instituto Mundial de Energía de KPMG



La suscripción gratuita al GEI es una forma eficaz para que los ejecutivos de la industria energético obtengan la información más reciente sobre las tendencias de la industria y les ayuda a cumplir sus requisitos de formación continua. Los miembros reciben alertas tempranas e invitaciones a exposiciones de liderazgo intelectual, estudios, eventos y *webcasts* sobre temas clave de la industria.

KPMG

European Power & Utilities Report

Insights on key trends in the European Power
& Utilities Industry

KPMG Global Energy Institute

Q4 2021



Servicios de seguridad cibernética de KPMG

Los profesionales de KPMG tienen un conocimiento profundo de los desafíos de la seguridad de la información en la industria de la energía y los recursos naturales (ENR), incluidos las TI y las OT dentro de la energía y los servicios públicos, el petróleo y el gas, las energías renovables, los productos químicos y la minería. Los Servicios Mundiales de Seguridad cibernética de KPMG son líderes premiados en el mercado de consultoría de seguridad cibernética.

Nuestras capacidades de seguridad cibernética son verdaderamente mundiales, con más de 3200 profesionales de seguridad de la información trabajando en firmas de KPMG de todo el mundo.

Los Servicios de seguridad cibernética de KPMG ofrecen un abordaje de cuatro pilares para presentar un conjunto de servicios coherente en todo el mundo. Estos servicios se alinean con las prioridades comerciales de los clientes para proporcionarles seguridad y ayudarlos a abordar los desafíos que enfrentan.

“
El GEI interactúa con sus más de 40.000 miembros por varios canales, incluidos webcasts, publicaciones y libros blancos.”



Estrategia y Gobernanza

Convierta el riesgo en una ventaja competitiva.

Ayudamos a los clientes a determinar los niveles adecuados de riesgo aceptable y a comprender la mejor manera de alinear su agenda cibernética con sus prioridades comerciales dinámicas y de cumplimiento.



Transformación

Acelere sus iniciativas en un entorno cambiante.

Ayudamos a los clientes a crear y mejorar sus programas y procesos, con el respaldo de la organización y la tecnología adecuadas, para mejorar su agenda cibernética.



Defensa Cibernética

Aproveche las oportunidades con confianza.

Ayudamos a los clientes a mantener su agenda cibernética a medida que sus programas comerciales y tecnológicos evolucionan, por medio de la entrega de una mayor visibilidad y comprensión de los riesgos cambiantes.



Respuesta cibernética

Opere con confianza en un mundo digital.

Ayudamos a los clientes a responder de manera efectiva y eficiente a los incidentes cibernéticos y a realizar análisis forenses e investigaciones detalladas. Una estrategia holística y adaptable alineada con sus objetivos comerciales.

→ **Alineado con las prioridades comerciales del cliente y las necesidades de cumplimiento** ←

Servicios en todos los pilares:

- Seguridad, resiliencia y transformación de la tecnología operativa
- Seguridad cibernética digital — Nube | Móvil | Internet de las cosas | Automatización inteligente | Blockchain
- Automatización segura



Anualmente, KPMG es identificado como líder en muchos informes de analistas clave que afectan los desafíos comerciales más apremiantes de los clientes.

Reconocimiento de la marca KPMG entre las firmas de consultoría de energía y recursos.

KPMG está calificada como la marca de consultoría de energía y recursos más conocida en una lista de las 15 principales organizaciones de consultoría del mundo. KPMG también obtuvo las mejores calificaciones de calidad de los clientes de energía y recursos. Este reconocimiento incluye el segundo lugar por la calidad del trabajo en datos y análisis y el tercero por la calidad del trabajo en gestión de riesgos (incluida la seguridad cibernética) por parte de clientes de la industria de energía y recursos.

Basado en 238 respuestas a una encuesta aplicada a clientes senior de firmas de consultoría y presentado en *Perceptions of Consulting in Energy & Resources in 2021*, publicado por Source Global Research.

La marca y los servicios de consultoría de riesgos de KPMG recibieron las mejores puntuaciones de los clientes actuales y potenciales.

KPMG ocupó el puesto número uno en “puntaje de marca actual” entre las firmas de asesoría de riesgos por la calidad de nuestros servicios de seguridad. KPMG recibió la puntuación más alta de los 16 proveedores evaluados en esta categoría, un gran logro determinado únicamente por los clientes actuales y potenciales. Esta clasificación se basa en la opinión compartida, nuestro nivel de credibilidad, autoridad y resiliencia competitiva, y encabezar esta calificación reconoce a nuestra marca como la más fuerte en la mente de los clientes en la actualidad.

Basado en 300 respuestas a una encuesta de clientes senior de firmas de consultoría y presentado en *Perceptions of Risk Firms in 2021*, publicado por Source Global Search.

Para obtener más información sobre Source y su investigación, visite: www.sourceglobalresearch.com.



Agradecimientos

Esta revista no sería posible sin la colaboración de colegas de todo el mundo que generosamente contribuyeron con su apoyo, conocimientos y puntos de vista en la planificación, análisis, redacción y producción de este informe. Gracias a Tzoulano Chotza, Lyndie Dragomir, Nicole Duke, Colleen King, Arun Mani, Michael Morihovitis, Michael Quigly y Peter Valentin.

Contactos

Regina Mayor

Directora Global de
Energía, KPMG
International
E: rmayor@kpmg.com

Valérie Besson

Líder Regional de Energía y Recursos
Naturales para Europa/Oriente Medio/África
(EMA) y Líder Nacional de la industria, Energía
y Servicios Públicos de KPMG en Francia
E: valeriebesson@kpmg.fr

Manuel Fernandes

Colíder Regional de Energía y Recursos Naturales
para las Américas y Líder Nacional de Petróleo y
Gas de KPMG en Brasil
E: mfernandes@kpmg.com.br

Ronald Heil

Líder mundial de seguridad
cibernética para energía y recursos
naturales KPMG en los Países
Bajos
E: heil.ronald@kpmg.nl

Angela Gildea

Colíder Regional de Energía y Recursos Naturales
para las Américas y Líder Nacional de la industria,
Energía, Recursos Naturales y Productos Químicos
KPMG en los EE. UU.
E: angelagildea@kpmg.com

Jonathon Peacock

Líder Regional de Energía y Recursos Naturales
para Asia Pacífico (ASPAC) y Líder de Petróleo y
Gas KPMG Australia
E: jjpeacock@kpmg.com.au

Algunos o todos los servicios descritos en este documento pueden no estar permitidos para los clientes de auditoría de KPMG y sus filiales o entidades relacionadas.

home.kpmg/pluggedin

home.kpmg/socialmedia



La información contenida en este documento es de carácter general y no pretende abordar las circunstancias de ningún individuo o entidad en particular. Aunque nos esforzamos por proporcionar información precisa y oportuna, no podemos garantizar que dicha información sea exacta a partir de la fecha en que se reciba o que seguirá siéndolo en el futuro. Nadie debe actuar sobre dicha información sin el asesoramiento profesional adecuado después de un examen exhaustivo de la situación particular.

© 2022 Propiedad de una o más de las entidades de KPMG International. Las entidades de KPMG International no proveen servicios a los clientes. Todos los derechos reservados.

KPMG se refiere a la organización global o a una o más de las firmas miembro de KPMG International Limited ("KPMG International"), cada una de las cuales es una entidad legal individual. KPMG International Limited es una empresa privada inglesa limitada por garantía y no brinda servicios a los clientes. Para obtener más detalles sobre nuestra estructura, visite home.kpmg/governance.

El nombre y el logotipo de KPMG son marcas registradas utilizadas bajo licencia por las firmas miembro independientes de la organización global KPMG.

En este documento, "nosotros", "KPMG", "nos" y "nuestro" se refieren a la organización global o a una o más de las firmas miembro de KPMG International Limited ("KPMG International"), cada una de las cuales es una entidad legal.

Diseñado por Evalueserve.

Nombre de la publicación: Plugged In

Número de publicación: 138193-G

Fecha de la publicación: Junio de 2022