



Creación de un futuro más seguro para el sector de servicios públicos

Introducción

Los productos de la industria de los servicios públicos (calefacción, energía, electricidad y tratamiento de aguas residuales) son la sangre que corre por las venas de todas las empresas del planeta, sin la cual nada funcionaría. Sin embargo, los incidentes de ciberseguridad de 2021 han demostrado que la industria de los servicios públicos es un creciente objetivo del ciberdelito y de las guerras informáticas.

La industria de los servicios públicos experimenta un proceso vertiginoso de cambios que no da indicios de desacelerarse. Además de la disruptiva transformación digital, la industria de los servicios públicos enfrenta la presión única de tener que transformar los mismos activos que produce. La descarbonización, la energía renovable, la eficiencia energética y la descentralización son la orden del día, y solo la tecnología más inteligente e innovadora puede hacerse cargo. A esto hay que añadir los numerosos requisitos de reglamentación que los operadores de servicios públicos deben equilibrar en un mercado global en crecimiento.

En este trabajo de investigación, examinaremos las principales tendencias que están transformando la industria de los servicios públicos en la actualidad y expondremos los desafíos y los riesgos que conllevan. Nuestra visión es la de un mundo donde los operadores de servicios públicos sean libres de maximizar la aplicación de tecnología inteligente que impulse la eficiencia, sin temer a la destrucción que pueden causar los ciberataques maliciosos.



Inteligencia artificial



Análisis de datos



Descarbonización



Recursos energéticos distribuidos



Desafíos regulatorios



Tendencia 1: Inteligencia artificial (IA)

La inteligencia artificial está cambiando la manera en que la industria consigue el suministro constante (y eficiente) del que dependen la reputación y los contratos de los proveedores. Estas tecnologías son posibles gracias al poder informático masivo a través de la nube, la proliferación de los macrodatos y la creciente sofisticación de la perspicacia algorítmica.

Por el lado de la producción, los operadores de servicios públicos aprovechan la IA para prever las cargas, optimizar la producción, analizar el consumo, predecir la demanda, prevenir el robo o la interferencia maliciosa, y ejecutar mantenimientos preventivos y tareas de reparación. Los operadores también buscan implementar estas tecnologías disruptivas para otras funciones empresariales, incluidas ventas, operaciones, atención al cliente, administración de las instalaciones, adquisiciones e informática.

Un uso común de la IA es el análisis de patrones meteorológicos históricos para calcular el impacto futuro en la red y en el comportamiento de los clientes, así como para asignar el equipamiento y la mano de obra necesarios para minimizar las interrupciones relacionadas con el clima. Los operadores están experimentando con drones no tripulados equipados con IA para recolectar información e imágenes del equipamiento de campo e identificar los riesgos de fallas de una manera mucho más eficiente que con las inspecciones manuales. También comienzan a notar el potencial papel de la IA en la coordinación de los recursos energéticos distribuidos, como la energía eólica, las baterías o la energía solar. Sin embargo, esto es solo el comienzo. Los servicios públicos cuentan con una enorme cantidad de información invaluable sobre los clientes y sus operadores tienen la capacidad de usar la IA para mejorar todos los aspectos relacionados con el compromiso con el cliente y para mejorar su modelo empresarial.

Usos de la IA para los servicios públicos:

- renovar la experiencia del usuario;
- agilizar las tareas de mantenimiento;
- anticipar cargas energéticas;
- integrar recursos energéticos distribuidos (DER);
- optimizar la generación, la transmisión y la distribución.



“Está a punto de ponerse en marcha una planta de energía que funciona con 'inteligencia artificial' en África Occidental. La unión empresarial entre la sede suiza de Xcell Security House and Finance y la sede estadounidense de Beyond Limits integrará inteligencia y conciencia de las operaciones, lo que aumentará la eficiencia, la productividad y las protecciones ambientales”.
[Forbes](#)

La IA también facilita la automatización robótica de procesos (RPA). La RPA es flexible, ampliable y adaptable a las necesidades específicas de cada servicio público. Reduce los costos y hace posible la mejora de servicios. También ayuda a abordar la escasez de mano de obra al administrar tareas simples para los clientes, como lecturas automáticas de medidores y algunos aspectos de control y cumplimiento reglamentario. Los servicios públicos transfieren rápidamente a la RPA los procesos sistemáticos rutinarios basados en reglas.

En la gran mayoría de los casos, los operadores de servicios públicos acuden a terceros para conseguir las tecnologías innovadoras que necesitan. Estos proveedores externos incluyen antiguas empresas líderes (como General Electric), así como empresas nuevas en la industria (como Open Energi). Veamos los siguientes dos ejemplos:

La granja eólica digital de General Electric recolecta de forma continua información sobre el clima, mensajes de los componentes, informes de servicio y rendimiento de modelos similares y la usa para construir un modelo predictivo que permita a los clientes mejorar el rendimiento, disminuir los riesgos y reducir el costo. En palabras de General Electric: “La granja eólica digital es un sistema de energía eólica de extremo a extremo que aprovecha los datos, el análisis y las aplicaciones de software, en conjunto con nuestras soluciones de hardware y servicios, para aumentar la eficiencia, ciberseguridad, fiabilidad y rentabilidad de los activos de nuestros clientes durante toda su vida útil”.

Open Energi “administra la energía distribuida para reducir de forma drástica los costos eléctricos y ofrecer una capacidad flexible que haga posible un sistema energético 100 % renovable”. La plataforma Dynamic Demand de Open Energi emplea IA para maximizar la utilidad de los activos, reducir los costos y optimizar el rendimiento. En julio de 2021, British Petroleum adquirió Open Energi y planea expandir su modelo empresarial a nivel mundial.



El foco en las amenazas: la IA es como la energía nuclear, “tan prometedora como peligrosa”. (Bill Gates)

Los riesgos de la IA son universales, independientemente de la aplicación: si se vulnera el sistema informático detrás de estas tecnologías, los sistemas que dependen de ellas sufrirán daños. El problema en la industria de los servicios públicos es que hay demasiado en juego. Sin electricidad, agua, tratamiento de aguas residuales, energía y luz, nuestra sociedad se derrumba. Esta precariedad se ve agravada por la inmadurez de estas tecnologías disruptivas.

El hecho de que la supervivencia de poblaciones enteras (ni hablar de las empresas) dependa del suministro seguro de agua, energía y gas convierte a las empresas de servicios públicos en objetivos llamativos, no solo de la ciberdelincuencia, sino de las guerras informáticas. Los agentes estatales entienden que paralizar los servicios públicos de un país desde la comodidad de una computadora malintencionada puede destruir más que cualquier

bomba. Un [estudio](#) reciente de Forrester reveló que el 88 % de los profesionales de la seguridad cree que los ataques movidos por IA se convertirán en la norma.

El 6 de mayo de 2021, se hizo un disparo de advertencia cuando Colonial Pipeline, el mayor oleoducto de Estados Unidos, detuvo todas sus operaciones como consecuencia de un ataque de ransomware, el cual se atribuyó a DarkSide, un grupo de hackers rusos.



Tendencia 2: Análisis de datos

Los datos son el combustible esencial que impulsa el avance tecnológico y digital en el sector de los servicios públicos. El sector de los servicios públicos está atravesando una revolución en la recolección y el análisis de datos en tiempo real a un ritmo cada vez más acelerado que hace posible la planificación y la toma de decisiones de forma proactiva. La analítica avanzada, junto con la experiencia humana, permiten que las empresas de servicios públicos no solo mejoren su compromiso con el cliente, sino que también administren mejor la cadena de suministro y el riesgo de la red, y mejoren las tareas de mantenimiento preventivo y planificación de activos. Para facilitar la recolección de datos, las empresas de servicios públicos instalan y mejoran las plataformas analíticas diseñadas para simplificar el uso y el seguimiento.

La medición inteligente es un área fundamental de las reformas energéticas. La tecnología está transformando la manera en que funcionan los servicios de energía, gas y agua para alcanzar nuevos y ambiciosos objetivos. La instalación de medidores inteligentes a escala global se está acelerando. Entre 2021 y 2025, más de 572 millones de [medidores de electricidad inteligentes](#) se instalarán en China, India, Japón y Corea del Sur. Los medidores inteligentes no solo les resultan interesantes a los consumidores, que pueden usarlos para disminuir el monto de las facturas de electricidad, sino que la gran cantidad de datos que recolectan también les permite a los proveedores impulsar la eficiencia desde el lado de la demanda como parte de la red eléctrica inteligente.

La red eléctrica inteligente es la contrapartida indispensable de la revolución de los medidores inteligentes. Para 2026, se espera que el mercado de la [red eléctrica inteligente mundial](#) supere los USD 92 000 millones. La tecnología industria de Internet de las cosas (IoT) se está implementando en toda la cadena de valor de los servicios públicos, desde la producción hasta la distribución y el consumo. Se prevé que el mercado de servicios públicos de IoT registrará ganancias de más del 20 % para 2024, según un informe de [Global Marketing Insights](#). Los sensores en los equipos de [centrales eléctricas](#), [instalaciones hidroeléctricas](#), [turbinas eólicas](#) y [paneles solares](#) permiten tomar decisiones informadas y, a veces, automáticas, lo que permite a los operadores ahorrar costos, optimizar los suministros y satisfacer la demanda. La recolección de datos ofrece un conocimiento invaluable para mejorar la seguridad y la resiliencia.



Un informe de Orbis Research sobre [los macrodatos globales en el mercado del sector energético](#) demostró cómo los macrodatos han ayudado a las empresas de servicios públicos a rastrear el patrón de consumo y la previsión, para cambiar en consecuencia el suministro tanto en tiempo como en espacio, lo que dio como resultado la utilización eficiente de los activos.



El foco en las amenazas: más dispositivos, más problemas (“en la guerra no se permiten los errores”)

Añadir dispositivos a una red es como agregar ventanas a un edificio. Cuantas más ventanas haya, mayor será el riesgo de intrusión (o de vulneración cibernética). También podemos decir que “cuantos más datos, más problemas”. Después de todo, los datos son a los ciberdelincuentes lo que el dinero a un ladrón. Cada herramienta de recolección de datos que se agrega a la red equivale a una superficie de ataque importante que se puede vulnerar.

La descarbonización también aumenta el número de puntos de intrusión de manera exponencial. Por ejemplo, se están conectando más dispositivos como las estaciones de carga de vehículos eléctricos todo el tiempo. Este escenario se ve agravado por el hecho de que la tecnología de esos dispositivos está en desarrollo y podría ser vulnerable a las amenazas cibernéticas más nuevas y desconocidas. Los servicios públicos que corren mayores riesgos son los que protegen un gran número de endpoints con recursos limitados. Las soluciones basadas en la nube permiten a los proveedores de servicios públicos interactuar con los clientes de nuevas maneras, pero traen problemas de seguridad adicionales.

Los riesgos son evidentes. Se estima que la vulneración masiva de [SolarWinds](#) afectó cerca del 25 % de los servicios energéticos de Estados Unidos en 2020-2021. Los ataques de ransomware subieron un 116 % en los primeros cinco meses de 2021, según la reseña de seguridad de [Nozomi Networks](#).

Para las empresas de servicios públicos, la inteligencia contra amenazas específicas de la industria es una parte vital de su equipamiento para la inmunidad cibernética. Solo la inteligencia experimentada puede ayudar a los operadores a adelantarse a las nuevas y desconocidas amenazas. También es fundamental el entrenamiento de recuperación ante crisis y respuesta ante incidentes. Además, con la proliferación de dispositivos y aplicaciones, los análisis del comportamiento y las anomalías desempeñan un papel crucial. Estas tecnologías de ciberseguridad combinan el análisis de datos y la IA para “conocer” el comportamiento de los usuarios con el objetivo de identificar y bloquear inmediatamente las anomalías que indican la presencia de cualquier amenaza, aunque aún sea desconocida.



“Las partes comparten una visión a largo plazo sobre la importancia de hacer realidad la totalidad del desarrollo y la transferencia de la tecnología, para mejorar la resiliencia al cambio climático y reducir la emisión de gases de efecto invernadero”.

Artículo 10 del [Acuerdo de París](#).

“El [sector energético de EE. UU.](#) se encuentra a mitad de camino de alcanzar cero emisiones netas, pero ahora es más complicado”.

Tendencia 3: descarbonización

Un informe de [McKinsey](#) hace referencia a la descarbonización de la industria como “la próxima frontera”. Por supuesto, si bien la responsabilidad de este proceso no recae solo en la industria de los servicios públicos, existe una relación natural entre ambos, y los operadores de los servicios públicos deben cumplir un papel fundamental. Para lograr la descarbonización, el informe de McKinsey recomienda que “el sector industrial y el sector energético refuercen su vínculo de manera significativa, debido a la interdependencia bidireccional”.

Las energías renovables y los recursos energéticos distribuidos (DER) cumplen un papel importante en la transición hacia la descarbonización. No obstante, es una tecnología en desarrollo que está haciendo posible el cambio climático a la escala que exige el planeta. Como parte del Acuerdo de París, firmado por 174 países y la Unión Europea, se incluyó la creación de un [Mecanismo tecnológico](#) administrado por la Convención Marco de las Naciones Unidas sobre el Cambio Climático ([CMNUCC](#)).

Si bien las energías renovables representan más del 20 % de la electricidad generada en Europa y Estados Unidos, los objetivos planteados son ambiciosos: un 33 % para 2025 y un crecimiento neto del 95 % de la capacidad energética global para 2050. Para afrontar el desafío de la descarbonización, se necesitan cambios muy profundos en la manera en que se desarrollan las operaciones de los servicios públicos. Esto supone la colaboración de los grupos de interés, la participación de los clientes y una enorme revolución tecnológica que implica digitalización, sensores, tecnologías de IoT y conectividad, que abarquen todos los aspectos de nuestras vidas con el fin de automatizar las iniciativas impulsoras de la eficiencia.

Se consideran clave estos tres desarrollos tecnológicos: el uso de vehículos eléctricos por sobre motores de combustión, la reducción del costo de generación y almacenamiento de energías renovables y la reducción del costo de la energía producida localmente para eliminar la necesidad de transporte de la energía. Todos los anteriores representan retos actuales para la industria energética.



El foco en las amenazas: “hipercomplejidad + hiperconectividad + hipervolumen de datos = hipervulnerabilidad” (UIT)

El programa [ONU Hábitat](#) estima que las ciudades consumen alrededor de un 75 % de la energía global primaria y emiten entre un 50 % y un 60 % de los gases de efecto invernadero del mundo, y la cifra se eleva a cerca del 80 % si se incluyen las emisiones indirectas generadas por sus habitantes. Las ciudades son los lugares clave para la aplicación de las nuevas tecnologías que las empresas de servicios públicos están adoptando cada vez más para cumplir las disposiciones y los requisitos del cambio climático.

Por desgracia, esto crea una tormenta cibernética perfecta, que la UIT describe como “hipercomplejidad + hiperconectividad + hipervolumen de datos = hipervulnerabilidad”. Las empresas de servicios públicos se encuentran en el ojo de la tormenta, navegando en innumerables dispositivos interconectados, acumulando y procesando enormes conjuntos de datos y enfrentándose a normativas cada vez más estrictas, que cambian a un ritmo vertiginoso.

La UIT mantiene esa ciberseguridad; la protección de la información y la resistencia de los sistemas son asuntos políticos y de gobierno. El informe de la UIT, sobre [ciberseguridad, protección de los datos y ciberresistencia en las ciudades inteligentes y sostenibles](#), destaca los potenciales efectos de los ataques malintencionados y de las catástrofes en la infraestructura y los sistemas de ICT críticos. Estos incluyen la privación de servicios esenciales para los ciudadanos, desde transporte hasta servicios públicos (por ejemplo, la red eléctrica inteligente y el tratamiento del agua).

La revista sobre tecnología emergente [Wired](#) predice que una infraestructura cada vez más conectada permitirá a los hackers derribar localidades enteras. Y las ciudades no hacen lo suficiente para estar preparadas.

Un [proveedor alemán de seguridad basada en la nube](#) señaló a la industria energética como el principal objetivo de los ciberataques en 2019, con una atracción del 16 % de los ataques totales del mundo. Se prevén más ciberataques a las cadenas de suministros de baterías y energía solar. Se prevé que la integración masiva de las redes con recursos energéticos renovables distribuidos hará que las redes energéticas sean más vulnerables a los ataques. En un contexto de hiperconectividad e interdependencias inevitables con los sistemas gubernamentales y municipales, es absolutamente necesario contar con un perímetro de seguridad sólido para las empresas de servicios públicos.



Tendencia 4: recursos energéticos distribuidos (DER)

La incorporación por parte de los consumidores de los recursos energéticos distribuidos (DER) está a la par de la inevitable transición del carbón hacia las energías renovables y del eventual abandono del combustible fósil. De acuerdo con [las nuevas perspectivas energéticas de Bloomberg](#), “las decisiones energéticas de los consumidores, como la instalación de paneles solares en el tejado y el almacenamiento de energía mediante baterías ‘detrás del medidor’ (BTM) ayudan a dar forma a una red eléctrica cada vez más descentralizada en todo el mundo”.

Los recursos energéticos distribuidos (DER) implican la generación de energía renovable a nivel local, lo que elude la infraestructura nacional (o incluso regional) existente y, por lo tanto, depende en gran medida del grado de liberación dentro de los respectivos mercados energéticos. La descentralización afecta tanto a la distribución como a la generación. Implica el establecimiento de un flujo de energía bidireccional para proporcionar el marco mediante el cual los consumidores normales que tengan, por ejemplo, paneles solares en sus casas, puedan devolver cualquier exceso de energía a la red y asumir así la nueva función de “prosumidores”. [Según la Unión Europea](#), esto es posible mediante la red eléctrica inteligente, que “abre la posibilidad a los consumidores que producen su propia energía de responder a los precios y vender el exceso a la red eléctrica”.

En la reunión del G7 durante el verano de 2021, se señaló la importancia de los recursos energéticos distribuidos (DER) para abordar los desafíos climáticos y de seguridad. Los DER facilitan la descarbonización al permitir el uso de energías renovables, por ejemplo, reemplazando la energía fósil por energía solar ([la energía solar mundial](#) creció en 2020 por la instalación de 138,2 GW, un crecimiento interanual del 18 %) y reemplazando el combustible por la electricidad con los vehículos eléctricos ([la venta mundial de vehículos eléctricos](#) creció un 41 % desde 2019 y la cuota de ventas de automóviles eléctricos a nivel mundial aumentó hasta un histórico 4,6 % en 2020). En todo el mundo, proliferan las soluciones de electrificación con un suministro de electricidad limpia y renovable en rápida expansión.

Bloomberg informa que “Australia y Japón están encaminados para desarrollar los dos sistemas eléctricos más descentralizados del mundo”. Estados Unidos también se encuentra en un rápido proceso de descentralización. En septiembre de 2020, la Comisión Federal Reguladora de Energía de EE. UU. (FERC) aprobó la [Resolución 2222](#), que abre las puertas para el mercado mayorista de recursos energéticos distribuidos (DER).



USD 96 700 millones

“Se prevé que el mercado global de bombas de calor crecerá de USD 60 400 millones en 2021 a USD 96 700 millones para 2026, con una tasa de crecimiento anual compuesto (CAGR) del 9,9 % para el periodo 2021-2026”. [Investigación y mercados](#)

Otra llamativa ventaja de los DER es que, al permitir una serie de soluciones energéticas eficientes y de demanda localizada mediante el uso de baterías y energía solar, ofrece un empoderamiento (en ambos sentidos de la palabra) a las poblaciones de los países en desarrollo, ya que les permite acceder, e incluso generar (como prosumidores), energía a nivel local, para evitar cualquier deficiencia en la infraestructura nacional, regional o local. El [Banco Mundial](#) calcula que 760 millones de personas en el mundo carecen de acceso a electricidad en sus hogares, cifra que se redujo de las más de mil millones de personas hace una década. “La electrificación mediante soluciones descentralizadas basadas, en particular, en energías renovables cobró impulso.” Sin embargo, la distribución entre países es sumamente desigual. De los ciudadanos de Sudán del Sur, solo el 6,7 % tiene acceso a electricidad; de Chad, el 8,4 %; de Burundi, el 11,1 %; de Malaui, el 11,2 %, y de la República Centroafricana, el 14,3 %.

Ahora bien, los DER resaltan la transición de las empresas de servicios públicos tradicionales que se esfuerzan por adaptar su modelo del siglo XX de grandes generadores centralizados y unidireccionales conectados a las redes que cubren la demanda estable y ofrecen una flexibilidad de precios casi nula. El flujo bidireccional de la energía es un desafío que podría llevar a un desbordamiento de la capacidad de las líneas eléctricas. Los dispositivos de uso final representan una carga para las redes que aún no es posible cuantificar. Que todos los consumidores enciendan las bombas de calor o carguen sus vehículos eléctricos al mismo tiempo podría causar picos de consumo de energía incontrolables. Cambiar al flujo bidireccional de energía significa forzar a las empresas de servicios públicos a realizar grandes inversiones para actualizar las redes eléctricas.



El foco en las amenazas: vulnerabilidades de las redes complejas automatizadas con varios nodos

La red eléctrica, y la infraestructura energética en general, no se diseñaron para el flujo bidireccional y sin duda tampoco para el flujo entre lugares de generación y distribución cada vez más reducidos. En lugar de un flujo unidireccional de energía preciso y con un control riguroso desde la red hasta el hogar (o la oficina), la descentralización crea una red interconectada de nodos finales de alta complejidad, controles avanzados, sensores digitales, arquitecturas de software y de red, con sus propias vulnerabilidades y potenciales problemas de seguridad con las conexiones. A esto se suma el hecho de que las redes tan complejas como esta dependen cada vez más de la automatización para funcionar, lo que introduce más vulnerabilidades relacionadas al uso de IA en hardware y software tradicional.

Las centrales eléctricas virtuales que usan una infraestructura de red eléctrica inteligente para conectar pequeñas cantidades de activos energéticos a un solo generador potencian a los consumidores como proveedores (prosumidores) que canalizan el exceso de energía hacia la red eléctrica inteligente. El modelo es atractivo y la industria energética prevé que habrá un aumento masivo de dispositivos digitales descentralizados dirigiendo el suministro de energía distribuido hacia las centrales eléctricas virtuales. Sin embargo, depender de una infraestructura de red eléctrica inteligente incrementa de manera notable el riesgo de ciberseguridad. Como las fuentes de energía generalizadas y descentralizadas se alimentan de los endpoints conectados a la red, el proceso centralizado de las centrales eléctricas virtuales es vulnerable a que los ciberdelincuentes accedan a toda la red desde un solo endpoint. Por ejemplo, un atacante podría, en teoría, alterar un número significativo de baterías de almacenamiento o cargadores de automóviles eléctricos como venganza. No es casualidad que estén en aumento el malware y el ransomware dirigidos a los servicios de infraestructuras críticas. El control de riesgos convencional ya no es suficiente. Los DER disminuyen claramente el control y la supervisión que las empresas de servicios públicos solían tener sobre los recursos energéticos almacenados en sus redes eléctricas.

Supervisar esta nueva red es un desafío complicado, agravado por la inmadurez del sector descentralizado. El sistema actual ofrece muy poca transparencia a los servicios públicos. Es evidente la necesidad de normas y regulaciones universales sólidas. También son importantes las preguntas acerca de la responsabilidad en la ciberseguridad.

Estos riesgos hacen que los análisis de vulnerabilidades específicos del sector y los acuerdos anticipados de respuesta ante emergencias sean imprescindibles para las empresas de servicios públicos. Es mejor prevenir que curar y, si ocurre lo peor (quizás debido a una vulnerabilidad dentro de una arquitectura independiente, pero conectada), actuar de forma rápida y adecuada puede detener el desastre.



Tendencia 5: desafíos regulatorios

Dada la naturaleza esencial de los servicios públicos, la industria se encuentra entre las más reguladas del planeta, sujeta a una extensa serie de reglamentaciones a nivel internacional, nacional, regional y local. Una gran proporción de estas reglamentaciones está relacionada con el hecho natural de que las empresas de servicios públicos suelen ser monopolios, en especial en países donde las empresas privadas han garantizado la licitación por el suministro exclusivo de servicios públicos regionales (o incluso nacionales). Sin embargo, las reglamentaciones relacionadas con los monopolios son solo el principio. Los operadores de servicios públicos deben lidiar con reglamentaciones que comprenden diversos problemas, incluidas operaciones, distribución, mantenimiento, interconexión, facturación y fijación de precios, competencia, adquisición, protección de datos y la mitigación del cambio climático. El incumplimiento de estas normas supone un aumento del riesgo para el sistema y multas económicas importantes.

No es sorprendente que la ciberseguridad y la resiliencia se controlen con tanta rigurosidad en la industria de los servicios públicos. Por ejemplo, la Comisión Federal Reguladora de Energía de EE. UU. exige que los operadores proporcionen respuestas detalladas acerca de su riesgo de resiliencia único, probabilidad de impacto, identificación de amenazas, planificación ante incidentes, mitigación de amenazas, análisis de eventos pasados, equipos, ingeniería y activos físicos. En todos los casos, los riesgos cibernéticos aparecen junto a eventos naturales como las sequías, desde la [Resolución de la FERC de enero de 2018](#).

“A medida que las empresas energéticas adaptan su modelo empresarial al entorno acelerado del mercado actual, también deben adaptarse sus funciones legales y de cumplimiento. La habilitación digital de los procesos de regulación y control del cumplimiento de la reglamentación energética puede ayudar a resolver esos problemas y cuestiones mediante una solución unificada”.
[Deloitte](#)

En 2021, los gobiernos de todo el mundo buscan con urgencia medidas para implementar resiliencia cibernética en empresas de servicios públicos fundamentales. El 6 de mayo de 2021, el ataque a [Colonial Pipeline](#), presuntamente perpetrado por un grupo de ciberdelincuentes con sede en Rusia, cerró 5500 millas de tuberías que transportaban el 45 % de los suministros de combustible de la costa este de EE. UU. Se declaró un estado de emergencia en cuatro estados de EE. UU. Para los reguladores fue un llamado de atención. ¿Hubo falta de cumplimiento? ¿Era posible prever este ataque? El Departamento de Seguridad Nacional dispuso más requisitos de ciberseguridad con rapidez “para una mejor identificación, protección y respuesta ante las amenazas a las empresas críticas del sector de oleoductos”.



“Los CEO informan la presión regulatoria en temas medioambientales, sociales y gubernamentales en una encuesta”.

[KPMG](#)

En la actualidad, la Unión Europea está elaborando un proyecto de ley (que reemplazaría a la ley de 2018) para intensificar los requisitos de ciberseguridad para los proveedores de electricidad y energía. Mediante un enfoque distinto, la Comisión Federal Reguladora de Energía de EE. UU. (FERC) propone modificar la ley para ofrecer incentivos de subvención federal (recuperación de costos diferida) a las empresas eléctricas que implementen medidas de seguridad superiores a los estándares de la regulación actual.

Además, las regulaciones introducidas recientemente que no están relacionadas con la ciberseguridad tienen, sin embargo, un gran impacto en las demandas de ciberseguridad. Un caso concreto es el de la Resolución 2222 de la Comisión Federal Reguladora de Energía de EE. UU. (FERC), que podría transformar el sector energético al liberar el mercado a proveedores mayoristas de recursos energéticos distribuidos (DER).

En conclusión, la vulnerabilidad cibernética de los activos energéticos integrados de forma digital aún requiere pruebas más completas. **Una encuesta de KPMG develó que el 48 % de los CEO de empresas de servicios públicos creía que ser víctima de un ciberataque era una cuestión de “tiempo”, no de “probabilidad”.**



El foco en las amenazas: el incumplimiento de las regulaciones provoca resultados fatales

El incumplimiento de las regulaciones puede provocar dos resultados catastróficos. Primero, si las regulaciones proveen un marco de orientación para los estándares de ciberseguridad, su incumplimiento podría dar lugar a una vulneración devastadora. En segundo lugar, en cuanto a la regulación, los incumplimientos podrían llevar a la pérdida de la licencia. Ambas consecuencias pueden poner de rodillas a un operador de servicios públicos.

La insistencia en 2021 de los ciberataques a las empresas de servicios públicos en todo el mundo confirma la importancia del problema. Para destacar solo dos casos: en agosto de 2021, una vulneración a [T-Mobile](#) permitió el acceso no autorizado a la información personal de más de 50 millones de personas. En mayo de 2021, un ataque de ransomware forzó a [Volve](#), una empresa noruega de tecnología energética, a cerrar instalaciones clave de agua y de tratamiento de aguas residuales. Las consecuencias de vulneraciones como las anteriores obligan a los reguladores a aplicar normas más estrictas.

Las multas también son cada vez más costosas. En 2019, [Duke Energy](#) enfrentó una multa histórica de USD 10 millones por parte de las autoridades federales tras la exposición de amplios fallos de ciberseguridad que, al parecer, "suponían un grave riesgo" para la seguridad y la fiabilidad de la red eléctrica. La reciente Ley de Protección de Datos Personales de China (septiembre de 2021) contiene disposiciones detalladas que regulan la recolección, el uso y la protección de los datos, así como medidas estrictas en caso de incumplimiento de las disposiciones, incluida la posible suspensión de la actividad.

El incumplimiento no es el único desafío cuando se trata de las regulaciones. La vertiginosa variedad de normativas que afectan a los operadores de servicios públicos de todo el mundo, en el contexto de las consecuencias drásticas que podrían derivarse de su incumplimiento, resulta agotadora, especialmente para las empresas que operan en varios mercados. Esto se complica aún más por la constante aparición de nuevas tecnologías y la incertidumbre relacionada con las regulaciones que surgirán para controlarlas.

Para las empresas de servicios públicos, prepararse para las regulaciones también significa incorporar la ciberseguridad correspondiente al sector.

Resumen

Las cinco tendencias desarrolladas antes destacan las enormes oportunidades y desafíos que deberán afrontar las empresas de servicios públicos. Es indispensable no solo incorporar nuevas tecnologías, sino también protegerlas. Crear una cultura de inmunidad cibernética potenciará a las empresas de servicios públicos a aprovechar realmente los elevados niveles de conectividad y automatización, minimizará los impactos negativos y maximizará la rentabilidad de las inversiones. Para el acelerado y cambiante entorno actual, Kaspersky tiene soluciones y servicios personalizados, diseñados a la perfección, sustentados por nuestra inteligencia de seguridad líder en el mundo, para proteger los datos y la continuidad del trabajo de forma ininterrumpida contra amenazas avanzadas y ataques dirigidos, mitigando riesgos, detectando ataques de manera anticipada, neutralizando ataques en vivo y fortaleciendo la protección futura.

Kaspersky ofrece un **enfoque de ciberseguridad por etapas** diseñado para aclarar cuáles son el nivel de seguridad y las soluciones específicas que se adaptan a su organización. Los marcos de trabajo proporcionan un conjunto de fácil administración de medidas de protección contra amenazas que se coordinan entre sí sin inconvenientes para satisfacer las necesidades de cada organización individual y ofrecen una estrategia de ciberseguridad que garantiza una transición fluida de un nivel de madurez de seguridad de TI a otro cuando llegue el momento.

El enfoque de ciberseguridad paso a paso de Kaspersky



Ciberseguridad: nivel de madurez	Solución
<p>TI</p> <p>Organizaciones pequeñas sin un equipo de seguridad de TI especializado</p>	<p>¿Qué? <u>Kaspersky Security Foundations</u></p> <p>¿Cómo? Implementa seguridad para organizaciones de cualquier tamaño y complejidad de infraestructura y brinda una prevención automática administrada en la nube contra amenazas genéricas en cualquier dispositivo, VDI e infraestructura de servidor híbrido.</p> <ul style="list-style-type: none"> ▶ Endpoints: Proteja cada endpoint en su organización con <u>Kaspersky Endpoint Security for Business; Kaspersky Embedded Systems Security</u> ▶ Cloud: Beneficiarse de una seguridad sin límites con <u>Kaspersky Hybrid Cloud Security</u> ▶ Red: Proteja su perímetro con <u>Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway</u> ▶ Datos: Proteja información valiosa y confidencial con <u>Kaspersky Security for Storage</u> ▶ Gestión de seguridad: Acceda a conocimientos especializados con <u>Kaspersky Premium Support; Kaspersky Professional Services</u>
<p>Seguridad de TI</p> <p>Para organizaciones que necesitan defensas avanzadas, pero cuyos recursos de seguridad de TI especializados son limitados</p>	<p>¿Qué? <u>Kaspersky Optimum Security</u></p> <p>¿Cómo? Combate amenazas evasivas con una detección y respuesta efectivas en endpoints, además de un monitoreo continuo de la seguridad, pero sin costos prohibitivos ni complejidades</p> <ul style="list-style-type: none"> ▶ Detección avanzada: mejore el análisis de comportamientos de aprendizaje automático, aislamiento de procesos, inteligencia de amenazas y búsqueda automatizadas de amenazas* con <u>Kaspersky Sandbox, Kaspersky Threat Intelligence Portal y Kaspersky Managed Detection and Response Optimum.</u> ▶ Análisis e investigación: mejore la visibilidad de las amenazas y el proceso de investigación simplificado con <u>Kaspersky Endpoint Detection and Response Optimum.</u> ▶ Respuesta rápida: implemente opciones de respuesta automática dentro del producto, así como situaciones de respuesta guiada y administrada* con <u>Kaspersky Endpoint Detection and Response Optimum y Kaspersky Managed Detection and Response Optimum.</u> ▶ Concienciación en seguridad: equipe a los empleados con herramientas automatizadas en todos los niveles y desarrolle habilidades de ciberseguridad clave con <u>Capacitación de Kaspersky Security Awareness.</u> <p>*Con el respaldo de los especialistas de Kaspersky</p>

Equipo de seguridad de TI con experiencia y completamente formado o SOC dedicado

- Tiene un entorno de TI distribuido y complejo
- Es un objetivo que tiene altas probabilidades de sufrir ataques sofisticados y similares a APT
- Necesita estar protegido contra riesgos debido a los altos costos de los incidentes de seguridad y las filtraciones de datos
- Le preocupa el cumplimiento normativo

¿Qué?

[Kaspersky Expert Security](#)

¿Cómo?

Dominio total de los ciberataques más complejos y específicos

- ▶ **Equipado:** equipe a sus expertos internos para abordar los incidentes de ciberseguridad complejos. Puede beneficiarse con una solución de ciberseguridad unificada. [Kaspersky Anti Targeted Attack Platform](#) con [Kaspersky EDR](#) en su núcleo fortalece a su equipo con funciones XDR.
- ▶ **Informado:** enriquezca su fuente de conocimientos con inteligencia de amenazas y capacite a los expertos para hacer frente a incidentes complejos:
 - Integre la inteligencia de amenazas con disponibilidad inmediata a su programa de seguridad. [Kaspersky Threat Intelligence](#) le ofrece acceso inmediato a inteligencia de amenazas técnica, táctica, operativa y estratégica.
 - Con la [capacitación en ciberseguridad de Kaspersky](#), desarrollará las habilidades prácticas de su equipo interno gracias al trabajo con evidencia digital, análisis y detección de software malicioso, además de la incorporación de prácticas recomendadas para responder a incidentes.
- ▶ **Reforzado:** recurra a expertos externos para hacer una evaluación de seguridad o recibir soporte y respaldo inmediatos:
 - Aproveche el soporte inmediato del equipo de [Kaspersky Incident Response](#), que está formado por analistas e investigadores sumamente experimentados para resolver los incidentes de ciberseguridad de forma rápida, efectiva y definitiva.
 - Con [Kaspersky Managed Detection and Response](#), incorpore una segunda opinión y la experiencia en búsqueda de amenazas administrada de un socio confiable. Sus expertos internos de seguridad de TI tendrán más tiempo para reaccionar a los resultados críticos que requieren toda su atención.
 - Conozca la eficacia de su defensa contra posibles cibramenazas y sepa si ya es el objetivo inadvertido de un ataque invisible a largo plazo gracias a [Kaspersky Security Assessment](#).

Soluciones específicas

¿Qué?



Kaspersky **Fraud** **Prevention**

La función Autenticación avanzada permite que la autenticación continua sea fluida y reduce los costos de procesos de doble factor para los usuarios legítimos, al mismo tiempo que mantiene altas tasas de detección de fraudes en tiempo real.

El análisis de fraudes automatizado examina a fondo los eventos que se producen durante toda la sesión y los transforma en datos valiosos.

Protege el perímetro externo de cualquier empresa, por lo cual garantiza la seguridad y protección de los ciudadanos o clientes.



Kaspersky **Industrial** **CyberSecurity**

KICS ofrece un enfoque holístico de la ciberseguridad industrial que aporta valor a cualquier etapa del proceso de seguridad de tecnologías operativas del cliente, desde las evaluaciones de ciberseguridad y la capacitación hasta las tecnologías avanzadas y la respuesta ante incidentes. Un ecosistema de productos y servicios integrados permite proteger las capas de tecnologías operativas y los elementos de su organización, incluidos los servidores SCADA, las HMI, las estaciones de trabajo de ingeniería, los PLC, las conexiones de red e incluso los ingenieros, sin que ello afecte la continuidad operativa y la coherencia del proceso industrial.



Evaluación **de seguridad** **para SCI de** **Kaspersky**

Para las organizaciones preocupadas por el potencial impacto operativo en la seguridad de TI/TO, Kaspersky proporciona una evaluación de ciberseguridad con una preinstalación poco invasiva. Al suponer un primer paso decisivo en el establecimiento de requisitos de seguridad en el contexto de las necesidades operativas, también puede proporcionar información importante sobre los niveles de ciberseguridad, sin ningún despliegue posterior de tecnologías de protección.



Noticias sobre ciberamenazas: www.securelist.com

Noticias de seguridad de TI: www.kaspersky.com/blog

Threat Intelligence Portal: opentip.kaspersky.com

Tecnologías en un vistazo: www.kaspersky.com/TechnoWiki

Premios y reconocimientos: media.kaspersky.com/en/awards

Herramienta de Portafolio Interactivo: kaspersky.com/int_portfolio