Consideraciones de ciberseguridad para 2022

Actúa ahora, protege tu futuro

kpmg.es

Prólogo

La ciberseguridad debe centrarse en lo que se puede hacer, no en lo que no se puede hacer

El panorama de las amenazas es cada vez más amplio y complejo. Los ciberdelincuentes son más activos que nunca y utilizan herramientas y tecnologías cada vez más sofisticadas. En este contexto en constante evolución, creemos que los directores de Seguridad de la Información (CISO, por sus siglas en inglés) y sus equipos deben adoptar un rol como habilitadores: la ciberseguridad ya no es una mera cuestión de prevención. No consiste en indicar a las diversas áreas lo que no pueden hacer, sino en mostrarles lo que sí deben hacer, desde la perspectiva de seguridad.

El cambio de paradigma del CISO: de ejecutor a figura de influencia

Aunque una de las principales lecciones que hemos extraído de la pandemia es que algunos de los mejores equipos de ciberseguridad son capaces de adaptarse rápidamente para **permitir a sus organizaciones** trabajar de forma segura, eficaz y en remoto, la conclusión más general y estratégica es que este periodo ha hecho que las empresas se replanteen cómo se relacionan con sus clientes y cómo les prestan servicio en un entorno que da prioridad a lo digital. Este cambio de mentalidad para centrarse en el cliente ha derivado en una rápida transformación digital, que ha ayudado a los clientes a moverse al ritmo del negocio, de forma segura.

En este entorno dinámico, los profesionales de ciberseguridad están pasando de ser **ejecutores** en la organización **a adoptar un papel de influencia**. La alta dirección está tomando nota. Según el **CEO Outlook de KPMG para 2021**, una considerable mayoría de consejeros delegados (el 75%) cree que una estrategia de ciberseguridad sólida es fundamental para **generar confianza** entre los principales grupos de interés.

Pero en el contexto de la aceleración de la transformación digital —que aumenta los riesgos de un ecosistema de terceros en constante expansión— los equipos de ciberseguridad también reconocen el reto de proteger no sólo dicho ecosistema sino también las cadenas de suministro. De hecho el 79% indica que esto es tan importante como definir y construir las defensas de su propia organización.

La mayoría de los consejeros delegados (58%) considera estar bien preparados para un ciberataque. No obstante, casi todas las organizaciones consideran cada vez más inevitable sufrir algún tipo de ciberataque. Es por ello que los equipos de seguridad deben estar preparados para la posibilidad de sufrir algún incidente y para poder responder, recuperarse y restablecer la confianza lo más rápido posible, pudiendo mitigar así los daños ocasionados. En paralelo, deben reconocer que el riesgo en este entorno es totalmente móvil y cambiante. Desde el consejo de administración hasta la alta dirección y desde el *front-office* hasta el back-office, deben existir controles para proteger los activos de alto valor de la organización y de los clientes, las famosas «joyas de la corona».

A lo largo de los años —y sobre todo a raíz de la pandemia— se ha comprobado que la falta de preparación y la sobrerreacción pueden ser tan perjudiciales como el propio ataque. Por eso es tan importante contar

con una estrategia clara, un plan de contingencias enfocado a diferentes escenarios y comprender la magnitud de los posibles incidentes. Se trata de una oportunidad para que las organizaciones de todos los sectores revisen sus estrategias de respuesta y recuperación y tengan una seguridad verdaderamente a prueba de errores.

En el horizonte: Ocho consideraciones para el CISO

Los CISOs deben desempeñar varios roles a la vez, pero no pueden estar en todas partes en todo momento. Si bien es importante recordar la tan repetida máxima de que «la seguridad es tarea de todos», es aún más importante reconocer que la seguridad es clave para crear y mantener la confianza de los clientes y los distintos grupos de la organización.

De cara a 2022 y en adelante, nos centraremos en ocho temas fundamentales que creemos que los CISOs deben priorizar a nivel de la alta dirección y el consejo de administración. Estos temas, enmarcados en un contexto normativo siempre cambiante, pueden ayudar a los ejecutivos a entender mejor cómo la ciberseguridad puede apoyar al negocio con un plan basado en la responsabilidad compartida.

Ya sean amenazas persistentes avanzadas, **ransomware**, ataques encubiertos o situaciones desconocidas, es probable que siempre haya nuevos riesgos a los que enfrentarse. Pero si los CISOs y sus equipos se centran en un conjunto de principios diseñados con los objetivos clave de la organización en mente, y si el plan está actualizado y es suficientemente flexible, podrán sin duda preparar a las organizaciones para mitigar el impacto de los potenciales ataques.

Marc Martinez

Socio Responsable de Ciberseguridad y Riesgo Tecnológico, KPMG en España

KPMG ha identificado

Ocho consideraciones clave de ciberseguridad para 2022

Haga clic en los temas para obtener más información.

Evolución de la respuesta a incidentes

Trabajar en el terreno de la prevención y la preparación, incorporando capacidades de análisis de amenazas e inteligencia.

Ampliar la conversación sobre seguridad estratégica

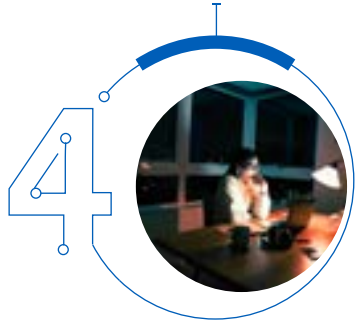
Cambiar la conversación entorno a los costes y la velocidad de respuesta hacia la seguridad efectiva para ayudar a generar mayor valor y mejorar la experiencia de usuario.

Adaptar la seguridad a la nube

Mejorar la seguridad cloud mediante la automatización, abarcando desde la implantación y la monitorización hasta la remediación.

Situar la identidad en el epicentro del enfoque Zero Trust

Aunar la gestión de identidades y la filosofía ZT en el contexto del trabajo hiperconectado y deslocalizado.



Aprovechar la automatización

Utilizar la automatización entorno a la ciberseguridad para ayudar a obtener valor de forma acelerada.

Privacidad desde el diseño y basada en tecnología

Pasar a un enfoque multidisciplinar, incorporando la privacidad y la seguridad desde el diseño y automatizando los principales procesos que componen este ámbito.

La seguridad de los terceros: clave

Transformar los enfoques de seguridad en torno a la cadena de suministro: de manuales y aislados, a automatizados y colaborativos.

Redefinir el alcance de la ciber resiliencia

Ampliar la capacidad operativa, poniendo foco en escenarios específicos, con el objetivo de recuperarse rápidamente y mitigar las consecuencias cuando se produce un ciberataque.

Consideración 1

Evolución de la respuesta ante incidentes

Trabajar en el terreno de la prevención y la preparación, incorporando capacidades de análisis de amenazas e inteligencia.

A medida que el panorama de las amenazas evoluciona, el enfoque de los equipos de ciberseguridad debe cambiar para intentar anticiparse

Con la pandemia en curso, las organizaciones están llegando a un punto en el que se espera que gestionen una mayor y más transversal presencia digital, donde la exposición de sus datos y activos críticos a través de múltiples canales, supone un desafío sin precedentes.

Adicionalmente, la tipología de amenazas a las que se enfrentan actualmente las compañías, se encuentran en un proceso de cambio, crecimiento, evolución y aumento de la complejidad que las convierte en una de las principales preocupaciones de los consejos de administración y de la alta dirección, situando a los equipos de seguridad en el punto de mira.

Contar con un proceso maduro de gestión de incidentes, capaz de gestionar cualquier brecha de seguridad o amenaza, resulta clave para garantizar la supervivencia de la empresa ante los potenciales efectos negativos derivados de una ataque, ya sea en términos de pérdida de recursos o impacto en la reputación corporativa.

Hacer el esfuerzo por estar preparados para afrontar cualquier tipo de amenazas puede ayudarnos a abordar escenarios que impliquen incluso el cese del negocio y afrontar la necesidad de contar, no solo con un buen plan de respuesta ante incidentes sino también con un **personal cualificado para poder hacer frente al mismo**. No se trata ya únicamente de una necesidad, sino de una obligación si queremos poder salir airosos ante situaciones inciertas.

Además, en los últimos tiempos ha quedado demostrado que la mayoría de empresas no puede confiar plenamente en la inviolabilidad de sus sistemas de seguridad, y están comprendiendo que es fundamental llevar un control más riguroso sobre la capacidad para proteger los datos y activos más críticos. Estamos viendo una clara tendencia por parte de los equipos directivos a exigir a las áreas de sistemas y de ciberseguridad que lleven a cabo simulacros de ataques con periodicidad para comprobar la solidez y actualización de sus procesos, así como el nivel de protección real y la capacidad de reacción ante desastres.

Esto requerirá más inversión y tiempo, pero proporciona a las empresas garantías de que están adecuadamente protegidas contra las ciberamenazas, y que son capaces de identificar las vulnerabilidades que deben ser eliminadas. Además, estos simulacros muestran si la organización tiene suficiente capacidad de respuesta en caso de sufrir un ciberataque, y si los sistemas de recuperación ante desastres funcionan adecuadamente.

Por otro lado, vemos cómo los ciberdelincuentes están virando progresivamente hacia los proveedores más pequeños, lo que provoca que los riesgos asociados a la cadena de suministro (con su potencial impacto geopolítico), o de terceros, sean casi inevitables. En este contexto, los ataques DoS (denegación de servicio) son altamente frecuentes por su capacidad para afectar a recursos transversales dentro de la organización (redes, maquinaria, sensores, equipos de trabajo, etc.) e imposibilitar el normal funcionamiento de los mismos.

Este tipo de incidentes incluyen también los provocados por sabotajes o ataques físicos a los recursos o infraestructuras.

Para ayudar a garantizar que los procesos de Incident Response sean eficaces y eficientes, algunas de las recomendaciones a tener en cuenta son:

a) Llevar a cabo análisis periódicos de madurez de las medidas de seguridad y procedimiento implementados por la compañía, poniéndolos a prueba mediante **simulacros o ataques dirigidos, basados en escenarios de recuperación**.

b) Invertir en recursos capaces de **contener las amenazas** una vez que se producen, de manera rápida y estratégica y que permitan recopilar información y evidencias asociadas al incidente en tiempo y forma

c) **Implementar evaluaciones de reingeniería de los procesos internos** para adaptarlos a los ataques de actualidad o con más riesgo para el negocio, poniendo el foco también en las tareas asociadas a ***Digital Footprint y Threat Intelligence*** para verificar que no se replica el incidente.

> “Moverse de un modelo reactivo a un modelo proactivo con respecto a las incidencias de ciberseguridad es un aspecto esencial para poder anticiparse a los atacantes en la medida de lo posible, puesto que el escenario de amenazas está en continuo cambio.
>
> El análisis de amenazas o los procesos de ciberinteligencia son los grandes aliados del proceso preventivo de la respuesta a incidentes.”

Sergi Gil
Socio de Ciberseguridad y Riesgo Tecnológico, KPMG en España

Algunas acciones clave para tener en cuenta para 2022

1. Es necesario cambiar el enfoque, si no se ha hecho ya: más proactividad frente a las amenazas en constante cambio, manteniendo la agilidad en la respuesta.
2. Realizar análisis periódicos de madurez simulando ataques de distintas tipologías y utilizando diferentes vectores.
3. Introducir tecnología que permita a los equipos de ciberseguridad enfocarse en acciones más estratégicas y relevantes.
4. Insistir en la concienciación de todos los miembros de la organización, incluyendo la alta Dirección para identificar posibles intentos de ataque y cómo actuar con diligencia y agilidad.
5. Incorporación de capacidades específicas de ciberinteligencia y threat hunting en el equipo de ciberseguridad de la organización.

Más información

Ciberincidentes: mirando más allá de lo obvio
Retos de incorporar la seguridad en desarrollo agile.

Adelántate a las brechas de ciberseguridad
Una ciber estrategia fuerte es clave para conseguir la confianza del cliente y el crecimiento del negocio.

Integración de la ciberserguidad a través de un CAU
Retos de integrar un CAU y la gestión de incidentes de seguridad.

Consideración 2

Ampliar la conversación sobre seguridad estratégica

Elevar el mensaje, ampliar los horizontes.

Los últimos dos años han redefinido nuestra forma de gestionar y hacer negocios. Asegurar y proteger los activos críticos, los sistemas y, sobre todo, la información sensible ya no es un problema exclusivo de los profesionales de seguridad e IT. Por el contrario, gestionar y mitigar el riesgo para ayudar a la viabilidad estratégica y operativa de toda la organización es una responsabilidad compartida que comienza por el negocio.

Aumentar la visibilidad del consejo de administración

Lograr una ventaja competitiva, una gestión proactiva y preventiva o alcanzar el éxito a largo plazo en materia de ciberseguridad, pasa inequívocamente por la **implicación, comprensión, apoyo y compromiso del consejo de administración y la alta dirección**.

Descargar la toma de decisiones estratégicas y la gestión del riesgo (especialmente el riesgo inherente a la digitalización) ya no es suficiente. Las soluciones de ciberseguridad modernas no pueden hacer mucho en términos de reducción de riesgos si los objetivos empresariales no incluyen **a la ciberseguridad como una apuesta clara y sólida** a todos los niveles de la organización.

Los CISOs, deben colaborar para crear un **entorno resiliente** mediante inversiones en ciberseguridad y apoyando los objetivos de crecimiento de la organización. Para ello, los equipos de ciberseguridad persiguen una serie de estrategias, entre las que se incluyen la **automatización** y la mejora de **procesos y tecnológicas de seguridad, el desarrollo de competencias** críticas para protegerse de la creciente escasez de talento y la creación de **modelos de ejecución que integren la seguridad y reduzcan los riesgos con partners y terceros**.

Para alinear mejor la seguridad con los objetivos estratégicos de la organización, los CISOs y sus equipos deben ayudar a los responsables de las áreas de negocio a comprender **las implicaciones de la seguridad y la privacidad desde el diseño**.

Esto implica, por tanto, cambiar la conversación del coste y el ritmo de despliegue a comenzar a hablar sobre **arquitecturas de ciberseguridad más efectivas** y destinadas a generar un mayor valor, mejorando la experiencia de usuario, **dando respuesta a los negocios** pero, a su vez, trabajando sobre unos **patrones modulares que permitan agilidad ante los retos de digitalización** o perspectivas cloud.

Las empresas deben encontrar un equilibrio. Está claro que la necesidad de respuesta de sus negocios hacia un mercado cambiante y demandante es muy elevada, pero es igualmente importante integrar la seguridad en los procesos empresariales de manera que permita a la organización mantener el ritmo, en lugar de crear un cuello de botella en el departamento tecnología o ciberseguridad.

El coste, en forma de pérdida de clientes, de inversores o de reputación puede ser sustancialmente mayor en el caso de no invertir el tiempo necesario para hacerlo bien.

Ampliar los límites de protección, la agilidad y la seguridad desde el diseño como columna vertebral del discurso ciber

Las tres **principales recomendaciones** en esta conversación **sobre la estrategia de ciberseguridad** las deberíamos centrar en:

1) ampliar los límites de protección, tanto de usuarios, como de datos y dispositivos (ya sean OT, IT, IoT…)

2) la ciberseguridad, al igual que el resto de áreas de las organizaciones, debe ser ágil para responder a los retos de un mercado cada vez más digital, cambiante y retador.

3) anticiparse a la regulación, trabajar desde las fases de diseño en embeber la ciberseguridad de manera proactiva.

Estos mensajes son los que deben calar en los consejos de toma de decisión, entendiendo que las **inversiones estratégicas en ciberseguridad, siempre serán más rentables que las reactivas o meramente operativas**.

> La ciberseguridad se vertebra a través de todos los procesos y negocios de la organización, el CISO es el guía pero la responsabilidad es compartida.
>
> En un mercado cada vez más digital y cambiante, la ciberseguridad debe ser ágil y estratégica a la vez, por lo que el rol del CISO juega un papel clave a la hora de exponer que las inversiones estratégicas en ciberseguridad, además de primar dicha agilidad, siempre serán más rentables que las reactivas o meramente operativas.
>
> **Javier Aznar**
> Socio de Ciberseguridad y Riesgo Tecnológico, KPMG en España

Algunas acciones clave para tener en cuenta para 2022

1. Transitar desde una visión de la seguridad tradicional hacia un modelo proactivo y preventivo, con foco en la resiliencia y en la protección de usuarios, dispositivos y datos en todo momento.

2. Los **grandes cambios a nivel tecnológico** que están experimentando las empresas requieren incluir la **seguridad desde el diseño** de esas estrategias, que en muchos casos parten desde negocio y que, si no se articulan así, provocan retrasos, riesgos innecesarios y falta de recursos.

3. Poner foco en la **seguridad de las terceras partes**. La dependencia de los negocios cada vez es mayor sobre terceras compañías, los impactos en protección del dato y la **disponibilidad de las operaciones** son muy elevados si no se controla y monitoriza de manera periódica el proceso end to end. **Evaluar, clasificar y actuar** deben ser prioridad.

4. En los últimos años ha quedado demostrado que las inversiones en **formación y concienciación en ciberseguridad** por grupos de empleados, ofrecen un ROI muy elevado. Los procesos de ciberseguridad siguen teniendo una alta dependencia del factor humano y muchos atacantes siguen pensando que este es el eslabón más débil.

5. Establecer **relaciones con las principales áreas de negocio** aumentando la concienciación sobre la rapidez con la que se pueden alcanzar los objetivos gracias a la **integración de la seguridad** frente a lo que pueden perder en caso de que exista un ataque o incidente.

Más información

Incorporar la ciberseguridad al ADN de la empresa
Los CISOs deben integrar la ciberseguridad en el negocio, haciendo que sea responsabilidad de todos.

Asegurar la nueva realidad empresarial
Los consejeros delegados de todo el mundo se enfrentan a sus miedos y a los riesgos de ciberseguridad.

Nuevo impulso a la ciberseguridad
Por qué la confianza es más importante que nunca.

Consideración 3

Adaptar la seguridad a la nube

Mejorar la seguridad en la nube mediante la automatización, desde el desarrollo y la monitorización hasta la remediación.

La ciberseguridad y la seguridad en la nube se están convirtiendo en sinónimos. La principal diferencia es el entorno de despliegue. La mayoría de principios y aspectos clave de la ciberseguridad —protección de datos, gestión de identidades y accesos, gestión de la infraestructura y las vulnerabilidades— son aplicables a la seguridad en la nube. El entorno en el que se despliegan estos controles de seguridad en la nube requiere una automatización mucho más amplia de la que estamos acostumbrados, desde el despliegue hasta la supervisión y la remediación. El «qué» y el «por qué» no han cambiado mucho, pero el «dónde» y el «cómo» sí lo han hecho.

La seguridad en la nube en la agenda de transformación digital

Si bien la **transformación digital impulsa la adopción y el uso de la nube**, también expone a las instituciones y empresas a un **mayor riesgo de ciberseguridad**. En muchos casos, la falta de competencias y conocimiento en materia de seguridad *cloud* significa que la actividad de protección de los principales procesos de negocio de la organización se enfrentan a riesgos que no están controlados. La nube puede estar en todas partes, pero también lo están los hackers y otros delincuentes.

En muchas empresas, existen ciertas expectativas con respecto a que el equipo de desarrollo cloud debe funcionar también como equipo de ciberseguridad. Eso no es realista ni sostenible. Lo ideal es que los profesionales de seguridad sean verdaderos expertos en esa disciplina crítica y tengan una **perspectiva relevante sobre la estructura básica y las necesidades del entorno de la nube**. Del mismo modo, los desarrolladores deben conocer en mayor profundidad el papel que juega la seguridad, y sin embargo, vemos cómo dedican la mayor parte de su tiempo a diseñar sistemas, desplegar, analizar, y mantener el entorno virtual sin tener la ciberseguridad en cuenta en las etapas más tempranas.

En lo que respecta a la ciberseguridad, las migraciones a la nube deben tener en cuenta y priorizar una amplia gama de factores normativos y contractuales. **En cuanto a la normativa, existe una verdadera amalgama de reglamentos —RGPD, EBA, Directiva NIS, PCI DSS, etc.— que siguen impulsando la complejidad en torno al cumplimiento normativo**, especialmente en lo que respecta a la seguridad, debiendo esto ser prioritario. En este escenario complejo y cambiante, **se anima a los equipos de seguridad a integrar herramientas que permitan ofrecer revisiones de políticas preconfiguradas** y asignadas a reglamentos específicos para ayudar a identificar los problemas de configuración relacionados con la nube y los riesgos asociados al cumplimiento.

En el ámbito contractual, tanto los proveedores de la nube como las empresas que utilizan sus servicios están suscribiendo acuerdos de responsabilidad compartida que a menudo se malinterpretan, especialmente por parte del cliente. Como resultado, la titularidad de la seguridad de la nube frente a la seguridad dentro de la nube puede ser un concepto poco claro.

Al hilo de esto, también vemos cómo **al pasar de la infraestructura como servicio (IaaS) al software como servicio (SaaS), el equipo de ciberseguridad es cada vez más dependiente de terceros**. En cualquier caso, la decisión de migrar a la nube está ya muchas veces tomada, por lo que se debe estar preparado para proteger los datos independientemente de dónde se encuentren definiendo planes de acción concisos y concretos.

Para ayudar a garantizar que los despliegues en la nube presenten el nivel adecuado de seguridad y que se adapten a la organización y a su perfil de riesgo, así como a sus características y funcionalidades, **una recomendación clara es capacitar al equipo de ciberseguridad con conocimientos amplios y específicos de ciberseguridad en la nube**. Una vez que la estructura y las competencias están aseguradas, este equipo puede distribuirse en unidades de negocio específicas o alinearse con ellas. Y de esta manera, continuar automatizando todo lo que pueda, cuando sea adecuado, particularmente en las áreas de despliegue, monitorización y remediación.

> “Es clave para las organizaciones contar con profesionales expertos en ciberseguridad en los entornos cloud, de manera que las migraciones a los mismos se hagan de manera segura, eficaz y asumiendo los mínimos riesgos posibles, sin perder de vista el importante papel que juegan los proveedores de estos servicios.”

Sergio Gómez
Director de Ciberseguridad y Riesgo Tecnológico, KPMG en España.

Algunas acciones clave para tener en cuenta para 2022

1. Automatizar en lo **posible la gestión de la seguridad en la nube**, especialmente en lo que respecta a la implantación, la supervisión y la remediación, sustituyendo los procesos manuales progresivamente.
2. Estructurar un **equipo de ciberseguridad en la nube especializado**, valorando que pudiera tener conocimiento previo en el despliegue o desarrollo de soluciones en la nube.
3. Fijar las **responsabilidades operativas**, incluyendo y especificando todas aquellas relativas a la seguridad en el entorno de la nube.
4. Buscar **herramientas de gestión de la configuración** de entornos cloud capaces de implantar controles asociados a políticas preconfiguradas en línea con diferentes Reglamentos, normativas y estándares de ciberseguridad.
5. Desarrollar un proceso de **respuesta a incidentes** que esté en sintonía con su estrategia general en la nube.

Más información

Asegurar la nube: siguiente capítulo
Cómo las soluciones actuales basadas en la nube están proporcionando beneficios y mitigando los riesgos tecnológicos del negocio.

La ciberseguridad de manera ejecutiva
Adoptar un nuevo enfoque para la protección de las empresas en el mundo posterior a la pandemia.

Protección de datos en la nube
Habilitación de capacidades escalables de protección de datos en la nube

Consideración 4

Situar la identidad en el epicentro del Zero Trust

Activar la relación entre la gestión de identidades y el paradigma Zero Trust

Con decenas de millones de empleados teletrabajando, y miles de millones de consumidores que compran productos desde sus teléfonos en cualquier lugar del mundo, la protección de los datos críticos y otros datos sensibles dentro de un complejo escenario de proveedores y partners nunca ha sido tan esencial. En un entorno en el que los ciberdelincuentes están a menudo a sólo un clic de distancia, las organizaciones deberían plantearse la posibilidad de adoptar una mentalidad y una arquitectura Zero Trust, teniendo en cuenta la gestión de identidades y accesos como parte de la estrategia.

Experiencia de usuario transparente y mejorada

La transformación digital venía ganando terreno antes de que el COVID-19 paralizase el mundo, y aún así, la pandemia aceleró ciertos procesos de forma radical. Las empresas y los consumidores se han visto empujados a entornos donde los canales tradicionales están migrando a canales digitales. Los empleados quieren acceder a las aplicaciones corporativas de manera deslocalizada a nivel geográfico y desde cualquier dispositivo.

Adicionalmente, los clientes, proveedores y usuarios corporativos esperan experiencias ágiles y agradables, sin el obstáculo de contraseñas que no paran de cambiar y múltiples capas de identificación digital, generando un reto más para los equipos de seguridad.

Toda esta complejidad **desafía las barreras tradicionales de seguridad basada en el perímetro**, convirtiéndolas en obsoletas y demostrado este enfoque es insuficiente puesto que los atacantes lo traspasan con facilidad y pueden llegar a realizar movimientos laterales sin ningún tipo de complejidad.

Esto ha llevado al desarrollo de un nuevo modelo de ciberseguridad conocido como "confianza cero" (Zero Trust - ZT). Un enfoque centrado **principalmente en la protección de datos**, pero que puede y debe expandirse para incluir todos los **activos** de la compañía como **dispositivos** *endpoints*, componentes de **infraestructura**, elementos *cloud*, **proveedores**, usuarios finales, **aplicaciones** y otros sistemas que solicitan información de recursos internos o externos.

Se trata de un paradigma de ciberseguridad y gestión de riesgos que **protege sin importar dónde se encuentren los datos y sus usuarios, orientado además a ayudar a eliminar procesos manuales** incluyendo la automatización a la hora de establecer nuevas políticas y procedimientos de ciberseguridad.

Teniendo en cuenta la identidad en la estrategia, permite a las organizaciones evaluar si un usuario está correctamente autenticado; aislar el recurso al que el usuario intenta acceder; determinar si la solicitud procede de un dispositivo de confianza, robado o de terceros; y decidir con seguridad si se debe conceder o no el acceso.

La aparición del Zero Trust representa un cambio de mentalidad en **el que el equipo de ciberseguridad asume la responsabilidad de validar los accesos a los sistemas**, tomando decisiones en tiempo real y que ponen en el centro la identidad, el dispositivo, los datos y el contexto.

De esta manera, tan solo se solicitarán mecanismos de doble factor de autenticación en aquellas situaciones donde se sospeche que pueda tratarse de un usuario potencialmente malicioso o fraudulento. En el resto de situaciones, se permitirá a los usuarios acceder a recursos corporativos sin experimentar ningún tipo de fricción en la experiencia de usuario, y siendo partícipes de una seguridad silenciosa y por defecto.

Por tanto, se debe tener en cuenta que la **implementación de un modelo ZT implica un proceso de transformación** más que un reemplazo de infraestructura, tecnología o procesos. Las organizaciones deben buscar implementar gradualmente los principios de ZT, procesando cambios y soluciones de manera gradual pero completamente transversal.

> “El modelo Zero Trust es un enfoque holístico para la estrategia de ciberseguridad. Zero Trust aúna en un mismo concepto la intersección entre la identidad, los datos y los activos para implementar un entorno de control y permisos que responsa a las necesidades de los negocios y ciberseguridad de la compañía. Si Zero Trust es la finalidad, la Identidad es el medio para articularlo.”
>
> **Juan Manuel Zarzuelo**
> Director de Ciberseguridad y Riesgo Tecnológico, KPMG en España

Algunas acciones clave para tener en cuenta para 2022

1. Los clientes, proveedores y usuarios corporativos esperan experiencias sin fricciones, sin el obstáculo de contraseñas que no paran de cambiar y múltiples capas de identificación digital

2. La aparición del Zero Trust representa un cambio de mentalidad en el que el centro se base en la identidad, el dispositivo, los datos y el contexto

3. Tan solo se solicitarán mecanismos de doble factor de autenticación cuando se sospeche de un usuario potencialmente malicioso o fraudulento

4. Un modelo ZT implica un proceso de transformación más que un reemplazo de infraestructura, tecnología o procesos, siendo un proceso que requiere tiempo y que debe abordarse con planificación, partiendo de un análisis exhaustivo del punto de partida y de los requisitos que se quieren implementar.

5. Automatizar las funciones de seguridad para que los profesionales altamente cualificados puedan centrarse en actividades más estratégicas

Más información

¿Es la autenticación un elemento diferencial para las empresas?
Por qué necesitamos una autenticación sin fisuras para la infraestructura digital.

Todo el mundo puede adoptar el enfoque «Zero Trust»
Las arquitecturas sin perímetro suponen un verdadero reto para un entorno de amenazas tan cambiante como el actual.

Lograr la eficiencia de costes en la gestión de identidades y accesos
Un enfoque estratégico de la gestión IAM, con su correspondiente automatización, puede ayudar a reducir los costes operativos.

Consideración 5

Automatización de la ciberseguridad

Generar ventajas competitivas mediante la implantación de procesos automáticos en el ámbito de la ciberseguridad.

Aunque pudiera verse la automatización como la solución a muchos problemas, la experiencia demuestra que es necesario utilizar el pragmatismo para ponerla en marcha. Algunos de los mayores beneficios de la automatización se obtienen cuando se hace hincapié en las implantaciones diseñadas para ayudar a resolver los problemas del negocio: aumentar el talento humano disponible mediante una ejecución más eficiente de las tareas manuales; obtener una ventaja competitiva en áreas donde la agilidad es importante; y analizar grandes conjuntos de datos, a menudo no estructurados. En un mundo hiperconectado con una infinidad de herramientas disponibles, las organizaciones deben estar preparadas para el futuro, ya que el panorama de las ciber amenazas sigue expandiéndose y aumentando en complejidad.

Materializar el valor del negocio

Las empresas están **empezando a automatizar números elementos dentro del ámbito de la seguridad** y liberando recursos mediante la simplificación de tareas rutinarias y repetitivas. El trabajo que antes realizaban profesionales altamente cualificados, como el escaneo de vulnerabilidades, el análisis de eventos y el cumplimiento normativo, se está estandarizando y ejecutando automáticamente.

En situaciones en las que los conjuntos de datos son demasiado grandes y complejos, se ha comprobado que la automatización es tremendamente valiosa.

En el mundo de la ciberseguridad una de las aplicaciones principales consiste en acelerar el descubrimiento de indicadores de compromiso (IOCs) y patrones difíciles de identificar pero ya vistos en ataques anteriores o similares.

De hecho, **uno de los beneficios más claros de la automatización de tareas básicas y rutinarias es la capacidad de aumentar la eficiencia de centro de operaciones de seguridad (SOC)** al permitir a los analistas acelerar la detección de incidentes y los tiempos de reacción, agilizando la investigación de alertas y dándoles las capacidad de centrarse en el análisis de aquellas amenazas que sí requieran de la intervención humana.

Desde la perspectiva de DevOps, la automatización de la seguridad debe incorporarse a cada punto crítico en el SDLC, desde las necesidades de los usuarios y las revisiones de código seguro hasta la definición de amenazas y las revisiones de código fuente con la ayuda de productos centrados en el análisis de código de aplicaciones tanto estáticas como dinámicas (SAST y DAST).

Con el cambio a la nube, las organizaciones no tienen un control uniforme sobre las versiones de software y las características generales asociadas a este entorno. Y en este contexto, la automatización ha sido fundamental para evaluar el riesgo y definir nuevas líneas de actuación en consecuencia, según sea necesario. **En los entornos *multicloud*, la exposición de datos, los permisos asociados a cuentas mal gestionados, las conexiones de red no seguras, los ataques de *ransomware* y otros riesgos diversos, son las principales preocupaciones de las organizaciones**. De esta manera, resulta evidente que los marcos de seguridad automatizados pueden proporcionar mejor visibilidad y control.

> La creciente automatización experimentada a todos los niveles por las compañías, supone un verdadero reto a la hora de definir la estrategia de ciberseguridad. Las organizaciones deben trabajar por optimizar los procesos tradicionales, con el fin de minimizar las tareas manuales y repetitivas, reducir la latencia y ayudar a lograr la escalabilidad y la agilidad necesarias para proteger los activos críticos.
>
> **Guillermo González**
> Director de Ciberseguridad y Riesgo Tecnológico, KPMG en España

Algunas acciones clave para tener en cuenta para 2022

1. Los mayores beneficios de la automatización se obtienen al poner el foco en ayudar al negocio: ejecución más eficiente de las tareas manuales, obtener una ventaja competitiva agilizando procesos y analizando de forma eficaz grandes conjuntos de datos

2. Automatizar las tareas más básicas y repetitivas para optimizar el tiempo de los profesionales del equipo de ciberseguridad, permitiendo que se centren en tareas más importantes.

3. Generar marcos de seguridad automatizados que permitan proporcionar mejor visibilidad y control no solo de las infraestructuras tradicionales si no también de los entornos cloud

4. Incluir procesos automáticos que ayuden a garantizar la seguridad en los puntos críticos dentro del ciclo de vida del desarrollo de software

5. Adoptar un enfoque pragmático y simple, sin buscar soluciones extremadamente complejas y sin adquirir herramientas por defecto que no encajen en la solución del problema o incapaces de aportar el valor esperado

Más información

Adoptar la automatización:
Valor diferencial a nivel de negocio

Agile Security in cloud DevOps
Un enfoque a futuro para la ciberseguridad y el desarrollo software

Monitorización continua en ciclos de desarrollo seguro.
Primeros pasos para incrementar la confianza en el desarrollo de software

Consideración 6

Privacidad desde el diseño y basada en la tecnología

Pasar a un enfoque multidisciplinar, incorporando la privacidad y la seguridad desde el diseño y automatizando los principales procesos que componen este ámbito.

En muchas empresas, la ciberseguridad y la privacidad de los datos se consideran disciplinas diferentes y a menudo operan en compartimentos estancos. En un entorno en el que se recogen y utilizan tantos datos sensibles, la revisión de terceros, de los nuevos sistemas y de las nuevas aplicaciones exigen un enfoque multidisciplinar enfocado a la gestión del riesgo desde el punto de vista de la privacidad; un enfoque que aúne tanto privacidad como seguridad desde la fase de diseño hasta la gestión del cambio.

Considerar prioritarios los derechos individuales

Hoy en día existe una mayor concienciación y reconocimiento de los derechos individuales en relación con la información personal. Con la **avalancha de regulación global**, desde el RGPD en Europa hasta diversos regímenes individuales en Asia, Norteamérica y Sudamérica —especialmente la Ley General de Protección de Datos (LGPD) de Brasil, la Ley de Privacidad del Consumidor (CCPA) de California y otras leyes estatales de EE. UU. que están apareciendo, **así como otros ámbitos que afectan a la privacidad, como la regulación de la inteligencia artificial o la evolución de entornos digitales**, el foco de atención sobre derechos, **privacidad y seguridad**, es mayor que nunca.

Casi en tiempo real, se puede ver la evolución del entorno regulador en materia de privacidad de datos. Gobiernos y Reguladores reconocen que los **incidentes de privacidad** resultantes de las brechas forman, cada vez más, parte de un conjunto más amplio de incidentes de ciberseguridad. Además, se está exigiendo a las organizaciones que informen de las **brechas de ciberseguridad** con mayor anticipación, y de forma mucho más transparente, con independencia de si ha provocado o no un impacto en la privacidad.

La mayoría de las jurisdicciones a escala global ya han implantado la obligación de informar sobre brechas de ciberseguridad, y no sólo aquellas que tengan que ver con privacidad. Existe una tendencia casi universal en el sentido de que numerosos países / territorios han implantado normas y reglamentos sobre privacidad basados en derechos, con el fin de capacitar a la persona y devolverle el

control sobre lo que cede cuando comparte información personal. Con tantos reglamentos diferentes, sin embargo, **el entorno regulador es cada vez más difícil de abordar** y cumplir, **particularmente para empresas que operan en múltiples jurisdicciones**.

La privacidad desde el diseño

La verdadera gestión proactiva de la privacidad en las organizaciones pasa por la gestión del cambio desde el momento en que se conciben nuevos servicios, procesos o productos.

Abordar la privacidad en esas primeras etapas será una de las garantías de éxito, dando respuesta a las necesidades de los negocios y atendiendo los principios de responsabilidad proactiva y diligencia debida que reclaman los reguladores.

Foco en la automatización de procesos: la tecnología como vehículo

La **automatización es la clave**, especialmente para organizaciones que carecen de margen y recursos para gestionar áreas como la **identificación y la comunicación del riesgo de privacidad**. Del mismo modo, la gestión de las **actividades de tratamiento** y su correspondiente actualización, la realización de **análisis de riesgos y de impactos, la gestión de derechos y consentimientos**, las relaciones con terceras partes y **encargados de tratamiento o las transferencias internacionales** deben evolucionar dentro de un paradigma de cumplimiento hacia la **automatización de su gestión**.

> “Las estrategias de privacidad del futuro deberán incorporar un enfoque de privacidad desde el diseño, lo cual no es simplemente una filosofía, sino una mentalidad cultural y un cambio en la organización. El motivo es que la privacidad no es una disciplina legal aislada, sino un enfoque holístico a la protección de datos que aúna ciberseguridad, tecnología, ética y gestión de riesgos.”

Javier Aznar
Socio de Ciberseguridad y Riesgo Tecnológico,
KPMG en España

Algunas acciones clave para tener en cuenta para 2022

1. La presente década se postula como la que aplicará el cambio definitivo en la implementación de técnicas de inteligencia artificial y analítica sobre datos, en esta nueva era digital, necesitamos que las empresas jueguen un papel clave, apuntaos las ideas de ética y **transparencia digital**.

2. Desde el **diseño y por defecto**, pese a ser uno de los conceptos básicos que desarrollaba el Reglamento General de Protección de Datos, a nuestro entender, sigue siendo un campo donde seguir trabajando y poniendo foco.

3. En un mundo cada vez más conectado y global, es inevitable trabajar con transferencias de datos fuera de la Unión, para ello uno de los grandes caballos de batalla a afrontar debe ser la correcta **gestión de estos procesos**, aportando claridad y control sobre los mismos, **ofreciendo confianza tanto a los clientes como al regulador**.

4. Las diferentes soluciones tecnológicas y desarrollos específicos ofrecen múltiples capacidades para facilitar la gestión de los procesos de cumplimiento en materia de privacidad, no solo facilitando la labor del DPO sino también en la implementación de controles específicos para la protección, cifrado, anonimización o bloqueo de la información.

5. Ciberseguridad y privacidad caminan de la mano, ahondar en los procesos y mecanismos que garanticen la protección de los datos, la prevención de fugas de información y la correcta gestión de los incidentes, debe ser un must claro.

Más información

Tecnología en materia de privacidad: y ahora, ¿qué?
La evolución de la tecnología en materia de privacidad de los datos en la era de la automatización.

Un ejercicio de equilibrio: privacidad, seguridad y ética
Cómo puede ayudar la creación de una combinación correcta de datos a impulsar el crecimiento..

Responsabilidad corporativa sobre los datos: cómo salvar la brecha de confianza del consumidor
A medida que las empresas recopilan más datos personales, aumentan las preocupaciones del consumidor.
Aprender cómo pueden pasar a la acción las empresas para recuperar la confianza del consumidor.

Consideración 7

La seguridad de los terceros: clave

Instar al conjunto de la cadena de suministro a no perder de vista la ciberseguridad, al tiempo que se protege a la organización.

La continua transformación digital sigue teniendo una prioridad alta para empresas, tanto grandes como pequeñas. Convertirse en una organización que antepone lo digital implica un enfoque centrado en los datos, los cuales se comparten de forma constante en todo un entorno tecnológico complejo y conectado de partners y proveedores.

Esta fluidez de los datos entre diferentes organizaciones derivado de los servicios que se prestan entre ellas y hacia los clientes crea numerosas oportunidades para que los ciberdelincuentes pongan en peligro sistemas y datos. ¿Cómo pueden ayudar los CISOs a mantener seguras sus propias organizaciones, al tiempo que instan al conjunto de su entorno a ser ciberseguro?

Ciberseguridad del entorno: el estado actual de soluciones y obstáculos

La mayoría de las organizaciones han dejado de ser las entidades aisladas y monolíticas que muchos clientes llevan tiempo creyendo que son. En gran medida dependen operativamente de una cadena de suministro robusta, así como de una infinidad de proveedores tradicionales y no tradicionales que a menudo disponen de acceso directo a sistemas y datos del negocio. Aunque las normas regulatorias y los marcos de ciberseguridad pueden ayudar a minimizar el impacto de ciberamenazas asociadas a terceros, se dan situaciones en las que dichos terceros pueden carecer de obligaciones claras para establecer controles adecuados con vistas a proteger los datos de sus *partners*, provocando que la totalidad de la red sea vulnerable a ciberataques.

Además, entendemos que la gestión del riesgo derivado de los servicios que prestan los proveedores es un aspecto clave. Ya sea por requisitos legales, por necesidades de marcos de seguridad o buenas prácticas internacionales, pero **resulta fundamental desplegar un correcto proceso que garantice la seguridad de dichos terceros**.

Desafortunadamente, aunque esta forma de revisar la madurez de un tercero a través de un marco de confianza puede ofrecer una visibilidad del riesgo casi en tiempo real, consume demasiado tiempo y dinero para la mayoría de las organizaciones. Como resultado de ello, muchas empresas, proveedores externos e, incluso, reguladores, soportan una presión cada vez mayor para garantizar de manera continua la seguridad de sus entornos. Esto está abocado a convertirse en un reto mayor a medida que aumente la complejidad del entorno del proveedor, apareciendo por ejemplo cuartas partes, *shadow* IT, la ausencia de supervisión del proveedor de SaaS, etc. Como resultado, los CISOs se enfrentan a la difícil tarea de pasar de la estrategia basada en cumplimiento a un enfoque mucho más proactivo que sitúe la supervisión continua, el uso de soluciones basadas en IA/ML, la información sobre amenazas y el enfoque Zero Trust en el núcleo del modelo de seguridad de su entorno.

Consideramos prioritario establecer qué áreas deben involucrarse en la gestión de riesgos de terceros, siendo especialmente relevante que esta función tenga transversalidad, y a su vez suficiente capilaridad, a lo largo de la organización, de manera que se represente la necesidad de cubrir diferentes riesgos, que pueden ir desde los más relacionados con la Seguridad, hasta aquéllos más relacionados con Privacidad. Es por ello que **apostamos por ubicar estas funciones en áreas más transversales, que tengan una representación a alto nivel y en el que puedan participar diferentes áreas.** En concreto, se hace necesario valorar el que, dada la naturaleza y objetivo del modelo de seguridad de terceros, el área de riesgos lidere esta gestión segura de terceros.

> Es necesario plantearse un modelo robusto y transversal de gestión de riesgos en terceros que permita gestionarlos de manera ágil, entendiendo su criticidad para el negocio y las dependencias existentes, y que permitan incorporar posibles nuevos riesgos tecnológicos que se deriven de la implantación o evolución de nuevos procesos de negocio.

Sergi Gil
Socio de Ciberseguridad y Riesgo Tecnológico, KPMG en España.

Algunas acciones clave para tener en cuenta para 2022

1. Vigilar de cerca los requisitos regulatorios a medida que siguen evolucionando, poniendo además énfasis en la cadena de suministro
2. Considerar la monitorización continua de controles como manera de impulsar el cambio en el entorno tecnológico desde el cumplimiento hacia una visión de la seguridad más basada en las operaciones
3. Explorar oportunidades para automatizar y aprovechar IA/ML en enfoques de seguridad de la cadena de suministro para mejorar la seguridad y permitir a los profesionales capacitados en materia de seguridad que se centren en actividades más estratégicas.
4. No debe pasarse por alto la tecnología operativa (OT) de la cadena de suministro; a medida que siguen convergiendo los sistemas de TI y OT, es probable que los delincuentes pretendan atacar los sistemas de OT con vistas a comprometer los datos del negocio.
5. Pedir implementar medidas de seguridad consistentes en línea con la gestión del riesgo tecnológico, y no desde la perspectiva del simple mero cumplimiento.

Más información

La empresa en sentido amplio — cómo asegurar el futuro
Cambiando el rumbo hacia un entorno de terceros más seguro.

Cambios en el entornos de terceros
Adaptar el enfoque para ayudar a asegurar el entorno en evolución.

Agilizar la gestión de riesgos de terceros con IA
Incorporar un profesional de IA digital en sus labores de seguridad frente a terceros.

Consideración 8

Redefinir el alcance de la ciber resiliencia

Ampliar la capacidad operativa, poniendo foco en escenarios específicos, con el objetivo de recuperarse rápidamente y mitigar las consecuencias cuando se produce un ciberataque.

Dado el volátil entorno digital actual, en términos de resiliencia, se debería tener en consideración en qué medida entienden, prevén y están preparadas las empresas para recuperarse del potencial impacto de un incidente de ciberseguridad grave. Se sugiere a los CISOs y a sus equipos que entablen un diálogo con los máximos responsables donde se cuestione la idea de que la organización puede absorber un ciberataque sin consecuencias o, en el peor de los casos, recuperarse en unos días.

Se debe explorar la capacidad de proseguir con las operaciones habituales si la disrupción durase varias semanas, mientras que se gestionan aspectos tales como la gestión de la atención a los medios de comunicación, los reguladores y los clientes en general.

«Existe un plan»

Cuando se pregunta a los CEO cómo abordan la posibilidad de un ciberataque, la mayoría dice: «Existe un plan» y «Es una de las prioridades de la agenda del consejo de administración». La experiencia de los últimos meses sugiere que las preguntas más pertinentes son:

¿En qué medida está preparada la empresa para afrontar una interrupción de entre cuatro y seis semanas como resultado de un ciberataque? ¿Cómo afectaría al servicio al cliente? ¿Qué supondría para sus centros de atención telefónica y distribución? ¿Podría pagar las siguientes nóminas? ¿Podría pagar a los proveedores? ¿Cómo afectaría una interrupción a los requisitos regulatorios y legales de la empresa?

Una compañía resiliente en términos de ciberseguridad, debe tener la capacidad de proteger sus datos y sistemas IT y OT, así como de continuar con sus actividades y procesos, en caso de sufrir un ciberataque, que afecte negativamente la disponibilidad, integridad o confidencialidad de dichos sistemas, la información o servicios asociados.

El objetivo de la ciber resiliencia es por tanto mantener la capacidad de una organización para continuar su operativa de forma ininterrumpida. Esto significa hacerlo incluso cuando los mecanismos de protección han fallado, como durante una crisis o después de una brecha de seguridad. También incluye la capacidad de restaurar los procesos y actividades después de tales eventos, así como la capacidad de cambiar o modificar continuamente los mismos, si fuera necesario, ante la posibilidad de nuevos riesgos. Las operaciones de respaldo y recuperación ante desastres son parte del proceso de restauración.

Para lograrlo, las organizaciones han de desarrollar, internamente, una serie de sistemas y planes, que permitan la implantación de los procesos y mecanismos necesarios, y generar así, una adecuada reacción y protección de su negocio. Sin perder de vista que las áreas de seguridad de la información, continuidad del negocio y resiliencia operacional, deben trabajar conjuntamente, pues todas persiguen un objetivo común.

En este aspecto existen una serie de **principales recomendaciones** que ninguna compañía debería pasar por alto:

a) Desarrollar **acciones** para manejar un incidente, definir **roles y responsabilidades**, y establecer **métricas** para medir la efectividad de la respuesta.

b) Implementar una **estrategia basada en escenarios** y en estrategias de recuperación conectadas.

c) Realizar **simulacros** para verificar si la organización es capaz de manejar un incidente y coordinar a las partes interesadas para llevar a cabo una respuesta eficaz

d) Dar respuesta a incidentes bajo un enfoque doble: la **contención** de la amenaza, y la **investigación** del origen del incidente.

e) Llevar a cabo las acciones que permitan una **monitorización continua** para confirmar que no hay otros indicadores de compromiso o intentos recurrentes de ataque.

> La empresa debe desempeñar una función activa en términos de resiliencia digital: simulaciones de escenarios, conociendo dónde están las dependencias, así como planes estratégicos que permitan conocer lo que pueden hacer y lo que no. Definir escenarios, articular playbooks y ejecutar pruebas es el camino más aconsejable para tener una capacidad de ciber resiliencia madura.

Sergio Gómez
Director de ciberseguridad y riesgo tecnológico,
KPMG en España.

Algunas acciones clave para tener en cuenta para 2022

1. Los CISOs y sus equipos deben entablar un diálogo con los máximos responsables donde se cuestione la idea de que la organización puede absorber un ciberataque sin consecuencias o, en el peor de los casos, recuperarse en unos días.

2. El objetivo de la ciberresiliencia es por tanto mantener la capacidad de una organización para continuar su operativa de forma ininterrumpida. Esto significa hacerlo incluso cuando los mecanismos de protección han fallado

3. Las áreas de seguridad de la información, continuidad del negocio y resiliencia operacional, deben trabajar conjuntamente, pues todas persiguen un objetivo común.

4. Las organizaciones han de desarrollar acciones para manejar un incidente, definir roles y responsabilidades, y establecer métricas para medir la efectividad de la respuesta

5. Se debe dar respuesta a incidentes bajo un enfoque doble: la contención de la amenaza, y la investigación del origen del incidente.

Más informaicón

Las mil caras del ransomware
Cómo defenderse y responder a los ataques de ransomware.

Seguridad en un mundo hiperconectado
Cómo prepararse y reaccionar ante ciberataques dirigidos a infraestructuras críticas.

Cómo salvaguardar su entorno OT durante la «pandemia de ransomware»
El rostro cambiante del ramsomware.

Conclusión

En un futuro no tan lejano

De cara al futuro, es probable que la sociedad hiperconectada se enfrente a mayores riesgos de ciberseguridad en múltiples frentes globales, derivados de la continua evolución de las amenazas existentes. Claramente, los avances tecnológicos que impulsan los negocios, las comunicaciones y el entretenimiento conllevan nuevos riesgos. En este informe hemos examinado temas interesantes como la evolución del equipo de seguridad, la automatización de la función de seguridad, la privacidad de los datos y la seguridad en entornos tecnológicos. A continuación, analizamos varios retos emergentes en materia de ciberseguridad. Aunque ninguno de estos temas es nuevo, creemos que pronto se convertirán en áreas destacadas de atención para los profesionales del área de ciberseguridad en prácticamente todos los sectores industriales.

IIoT

A medida que sigue expandiéndose el **Internet de las Cosas Industrial** (IIoT), millones de sensores, máquinas y otros dispositivos conectados, basados en la nube, **podrían convertirse en puntos de entrada vulnerables de los ciberdelincuentes**. La urgencia desde una perspectiva de ciberseguridad estriba en que, debido a las prisas por innovar, el software empleado en estos sistemas hiperconectados a menudo no incluye los controles de gestión de riesgos apropiados.

Claramente, el **IIoT está creando un nuevo conjunto de superficies de ataque**. Aunque las prioridades de los fabricantes están cambiando, hasta el momento el diseño arquitectónico de los sensores en conexión con, por ejemplo, la calidad del aire, el tráfico, la gestión de los residuos y la red de energía en general, quizás no haya abordado plenamente la seguridad. Pueden existir graves restricciones operativas en dispositivos individuales en lo que respecta a limitaciones de potencia y peso que podrían interferir en la integración de controles, pero la seguridad de las infraestructuras no puede considerarse a posteriori.

Las organizaciones deberían centrarse en la profundidad a la que se integra la seguridad en los productos que habilitan el IIoT y la manera en que dichos dispositivos se integran dentro del entorno tecnológico en sentido amplio. En lo que respecta a la implantación estratégica de estos productos en un entorno empresarial o de ciudad inteligente, hablamos de una diversidad mucho más amplia de personas, políticas, procedimientos y tecnologías, así como consideraciones tales como la supervisión de anomalías, la gestión de identidades, enfoque Zero Trust, etcétera.

De cara al futuro, creemos que el **IIoT debería considerarse un componente esencial** dentro un ecosistema más amplio que, en última instancia, constituye una posición de seguridad de alcance **general.**

> “Es un círculo que se retroalimenta, en el que cada nueva tecnología amplía el panorama de amenazas y suscita la innovación en materia de ciberseguridad para ayudar a mejorar las capacidades de defensa. ¿Es esta carrera la única manera de operar? Creemos que integrar la seguridad en cada aspecto de TI, OT, y en cada proceso y procedimiento intrínseco al ADN de una empresa, es el futuro inevitable y la única salida.”
>
> **Sergi Gil**
> Socio de Ciberseguridad y Riesgo Tecnológico, KPMG España.

Hoy en día, la sociedad vive y realiza negocios en un mundo digital de datos, dispositivos y dependencia. La confianza se deposita en la tecnología de una forma que sería impensable hace una década, lo que plantea cuestiones de ciberseguridad, protección, privacidad…

Los profesionales de la ciberseguridad deben afrontar esta nueva realidad, ayudando a los principales responsables de las empresas a entender las consecuencias de depositar confianza en la tecnología y su resiliencia, anticipando simultáneamente cómo puede ser explotada dicha tecnología por terceros.

Esto puede aportar una perspectiva diferente y valiosa, pero también existe el deber de ofrecer un asesoramiento que sea pragmático y práctico.”

Marc Martínez
Socio Responsable de Ciberseguridad y Riesgo Tecnológico,
KPMG España.

Redes 5G

Las potenciales capacidades de conectividad que posibilitan aplicaciones emergentes basadas en redes 5G son emocionantes, pero estos ecosistemas conectados basados en *software* no solo deben priorizar la innovación técnica, sino también la seguridad de los dispositivos que pueden facilitar dichas conexiones.

Una red 5G es fundamentalmente diferente a la 4G en **términos de velocidad, ancho de banda, latencia y sofisticación en general**. Naturalmente, la 5G va a permitir enormes avances en conectividad, pero también conlleva un conjunto diferente de retos de seguridad y exige una arquitectura, supervisión y controles de seguridad altamente sofisticados. Algunas de estas preocupaciones introducen en la cadena de suministro internacional ciertas tensiones en relación con el aprovisionamiento de infraestructura y componentes tecnológicos.

Asimismo, se abre un debate interesante en torno a la confianza. Con 5G, los profesionales de ciberseguridad estarán probablemente en una posición en la que millones de dispositivos, cada uno con su propia identidad digital, podrían estar conectándose simultáneamente en entornos no fiables caracterizados por arquitecturas de conexión muy fluidas. **En nuestra opinión, este aire de impredecibilidad sugiere que las organizaciones deben asumir un criterio común y basado en el paradigma Zero Trust, así como una arquitectura de autenticación flexible y adaptable** a estas nuevas dependencias y problemas de resiliencia.

AI

Aunque ya es un área en auge, la IA —ML y aprendizaje automatizado en particular— probablemente seguirá siendo un aspecto atractivo en el futuro.

Obviamente, **la seguridad de aplicaciones de IA que realizan aprendizaje constituye un reto muy diferente a la ciberseguridad de sistemas convencionales**. Hay numerosas preguntas: ¿Está operando el software dentro de sus parámetros delimitados? ¿Qué grado de sesgo está presente? ¿Está siendo manipulada la aplicación por un agente malicioso o IA no controlada con vistas a poner en peligro información sensible? De cara al futuro, los profesionales del área de ciberseguridad también podrían tener que pensar en la integridad, la previsibilidad y la aceptabilidad de la aplicación de IA en el contexto del entorno operativo para el que se ha formado y diseñado. En este ámbito, es recomendable que los CISOs y sus equipos establezcan fuertes relaciones con el director de Tecnología y sus equipos de científicos de datos. En lo que respecta a la seguridad, este es un territorio nuevo.

En un futuro próximo, los ciberdelincuentes probablemente recurrirán también a la automatización robótica de procesos, ML y aprendizaje automático. **El sondeo y la evaluación de las vulnerabilidades y defensas de un entorno profesional está comenzando a automatizarse**, como ya se hace con la creación de campañas de correo basura o el acceso fraudulento al correo electrónico. Los atacantes están utilizando IA, pero no tienen límites. A corto plazo, es más probable que los delincuentes puedan aprovechar la IA para industrializar sus ataques. Ya está sucediendo y probablemente continuará.

A nivel regulatorio tenemos un **borrador de Ley de Inteligencia Artificial a nivel Europeo, que esperamos que a lo largo de 2022 termine de ver la luz** en su versión definitiva.

En este terreno, como en tantos otros, la regulación va a llegar un paso después, suponiendo la situación actual un riesgo relevante en materia de ciberseguridad.

Contactos

Marc Martínez
Socio Responsable de Ciberseguridad y Riesgo Tecnológico
KPMG en España

Sergio Gómez
Director de Ciberseguridad y Riesgo Tecnológico
KPMG en España
sergiogomezrodriguez@kpmg.es

Sergi Gil
Socio de Ciberseguridad y Riesgo Tecnológico
KPMG en España
sergigil@kpmg.es

Juan Manuel Zarzuelo
Director de Ciberseguridad y Riesgo Tecnológico
KPMG en España
jzarzuelo@kpmg.es

Javier Aznar
Socio de Ciberseguridad y Riesgo Tecnológico
KPMG en España
jaznar@kpmg.es

Guillermo González
Director de Ciberseguridad y Riesgo Tecnológico
KPMG en España
ggonzalezgonzalez@kpmg.es

Es posible que algunos de los servicios descritos aquí no puedan prestarse cuando se trate de clientes de auditoría de KPMG y de sus entidades afiliadas o vinculadas.

kpmg.es