Servicios de Consultoría

El camino hacia la resiliencia cibernética

Encuesta Global de Seguridad de la Información 2016-17

I Marzo 2017

EY
Building a better working world

Contenido

III. Respuesta ante incidentes

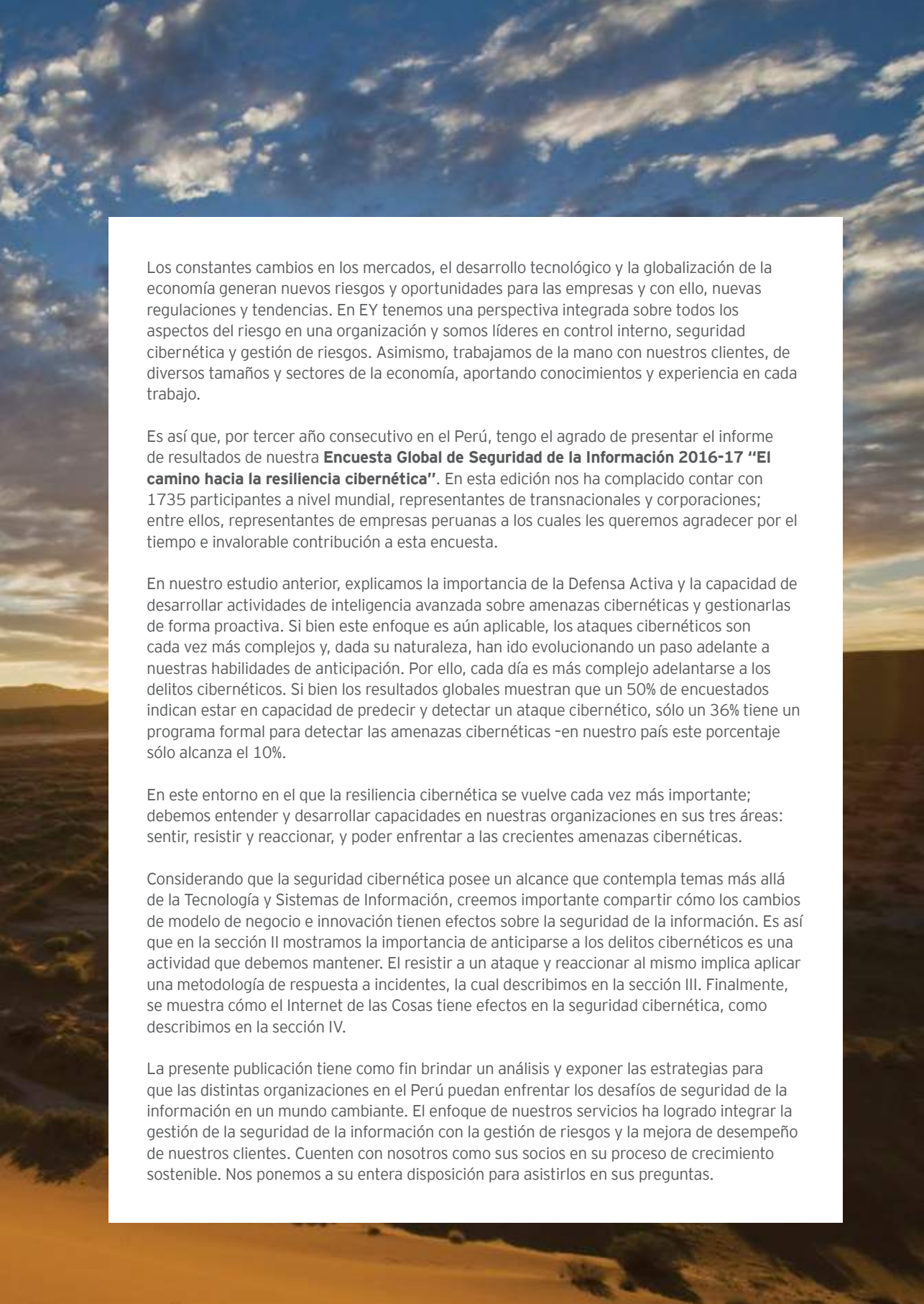
IV. Seguridad cibernética y el Internet de las Cosas

Contactos

Bienvenida

Jorge Acosta

Socio Líder de Consultoría



Los constantes cambios en los mercados, el desarrollo tecnológico y la globalización de la economía generan nuevos riesgos y oportunidades para las empresas y con ello, nuevas regulaciones y tendencias. En EY tenemos una perspectiva integrada sobre todos los aspectos del riesgo en una organización y somos líderes en control interno, seguridad cibernética y gestión de riesgos. Asimismo, trabajamos de la mano con nuestros clientes, de diversos tamaños y sectores de la economía, aportando conocimientos y experiencia en cada trabajo.

Es así que, por tercer año consecutivo en el Perú, tengo el agrado de presentar el informe de resultados de nuestra **Encuesta Global de Seguridad de la Información 2016-17 "El camino hacia la resiliencia cibernética"**. En esta edición nos ha complacido contar con 1735 participantes a nivel mundial, representantes de transnacionales y corporaciones; entre ellos, representantes de empresas peruanas a los cuales les queremos agradecer por el tiempo e invalorable contribución a esta encuesta.

En nuestro estudio anterior, explicamos la importancia de la Defensa Activa y la capacidad de desarrollar actividades de inteligencia avanzada sobre amenazas cibernéticas y gestionarlas de forma proactiva. Si bien este enfoque es aún aplicable, los ataques cibernéticos son cada vez más complejos y, dada su naturaleza, han ido evolucionando un paso adelante a nuestras habilidades de anticipación. Por ello, cada día es más complejo adelantarse a los delitos cibernéticos. Si bien los resultados globales muestran que un 50% de encuestados indican estar en capacidad de predecir y detectar un ataque cibernético, sólo un 36% tiene un programa formal para detectar las amenazas cibernéticas –en nuestro país este porcentaje sólo alcanza el 10%.

En este entorno en el que la resiliencia cibernética se vuelve cada vez más importante; debemos entender y desarrollar capacidades en nuestras organizaciones en sus tres áreas: sentir, resistir y reaccionar, y poder enfrentar a las crecientes amenazas cibernéticas.

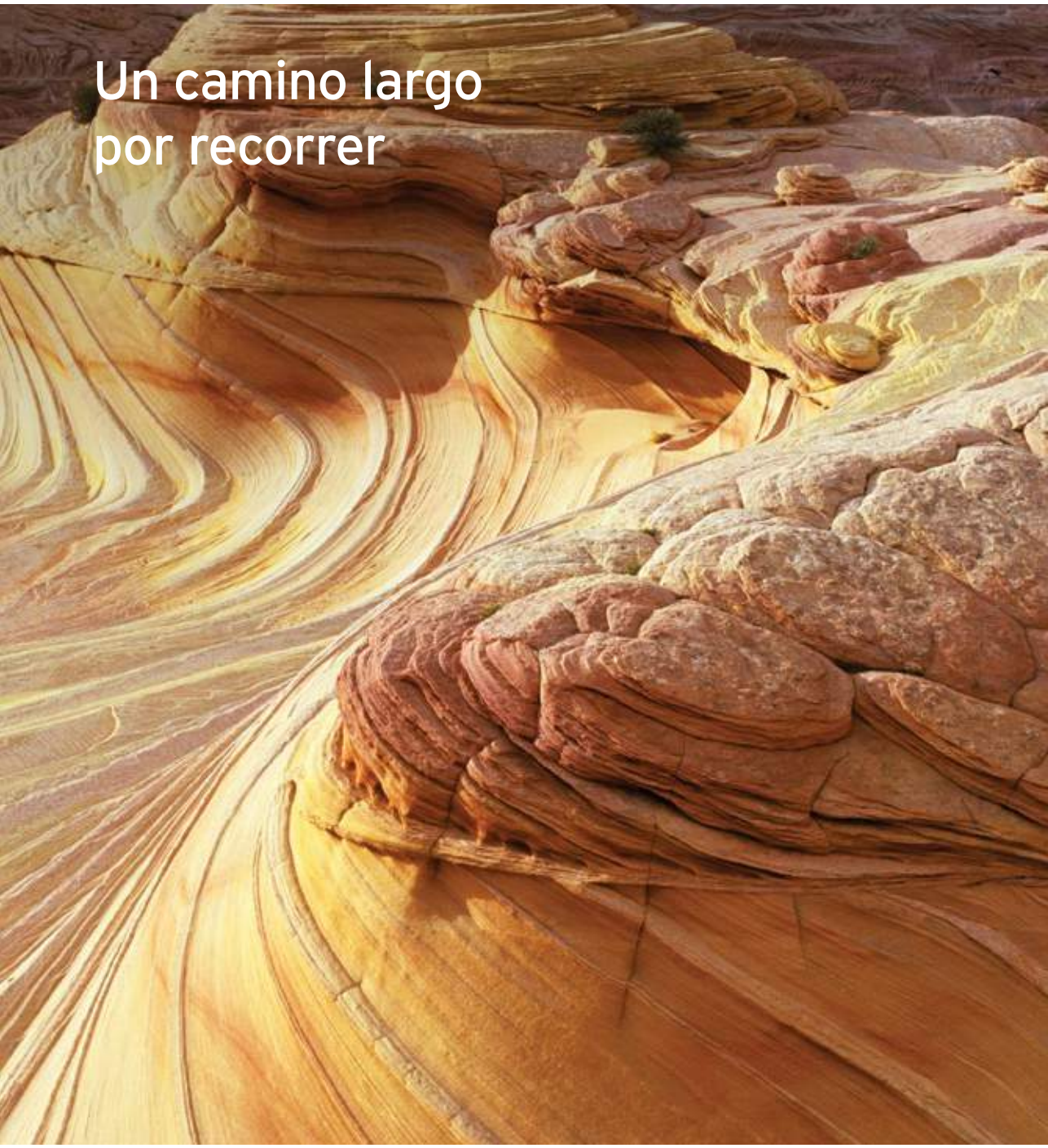
Considerando que la seguridad cibernética posee un alcance que contempla temas más allá de la Tecnología y Sistemas de Información, creemos importante compartir cómo los cambios de modelo de negocio e innovación tienen efectos sobre la seguridad de la información. Es así que en la sección II mostramos la importancia de anticiparse a los delitos cibernéticos es una actividad que debemos mantener. El resistir a un ataque y reaccionar al mismo implica aplicar una metodología de respuesta a incidentes, la cual describimos en la sección III. Finalmente, se muestra cómo el Internet de las Cosas tiene efectos en la seguridad cibernética, como describimos en la sección IV.

La presente publicación tiene como fin brindar un análisis y exponer las estrategias para que las distintas organizaciones en el Perú puedan enfrentar los desafíos de seguridad de la información en un mundo cambiante. El enfoque de nuestros servicios ha logrado integrar la gestión de la seguridad de la información con la gestión de riesgos y la mejora de desempeño de nuestros clientes. Cuenten con nosotros como sus socios en su proceso de crecimiento sostenible. Nos ponemos a su entera disposición para asistirlos en sus preguntas.

I.

¿Resiliencia cibernética o agilidad cibernética?

Introducción



Un camino largo por recorrer

Cuando hablamos con Directores, Gerentes Generales (*CEOs* por sus siglas en inglés) o Gerentes de Tecnología de la Información (*CIOs* por sus siglas en inglés), siempre hay mucho qué discutir respecto de la seguridad cibernética. ¿Está funcionando nuestra seguridad cibernética?, y ¿está operando bien? Se preocupan por tener presupuesto suficiente, un equipo con las habilidades adecuadas y las últimas tecnologías y, sobre todo, están realmente preocupados de ser víctimas de un gran ataque cibernético a pesar de todas las medidas que se han tomado para prevenirlo. La verdad es que todo el mundo necesita ayuda. Ya que todos estamos frente al mismo enemigo común, cuanto más compartamos sobre nuestras preocupaciones y experiencias, éxitos y fracasos, y cuanto más colaboremos en la búsqueda de respuestas, más aprenderemos y estaremos mejor protegidos.

Hay cosas que sabemos con certeza: la seguridad cibernética es una responsabilidad compartida dentro de una organización. Los altos directivos deben apoyar los esfuerzos que se están realizando, y cada empleado necesita aprender a mantenerse al margen de problemas, no abrir *mails* fraudulentos o que faciliten la obtención de información y cuidar su *smartphone*. Pero incluso teniendo todo esto, ¿estamos totalmente seguros?

Podríamos no querer admitirlo, pero la respuesta más probable es: no. Porque si hay algo más que usted debe saber, es que el diablo está en los detalles, y cuando se piensa en la seguridad cibernética que puede necesitar un ecosistema, nos referimos a una gran cantidad de detalles.

En este informe, examinamos los resultados de nuestra última **Encuesta Global de Seguridad de la Información**. Al revisar las respuestas de los 1,735 *CIOs*, *CEOs* y otros ejecutivos que generosamente compartieron su información, podemos ver en dónde las organizaciones tienen una gran fuerza y madurez en sus capacidades de seguridad cibernética, y creemos que hay algunas cosas muy específicas que las organizaciones pueden hacer.

- **Primero, afine sus sentidos.** ¿Puede ver al atacante cibernético acercándose a su perímetro de seguridad? ¿este perímetro existe? ¿sabría usted si alguien está empezando a socavar - o lanzar un ataque sobre - sus defensas? ¿podría detectar a un atacante escondido en una parte de su red remota?
- **Segundo, aumente su resistencia a los ataques.** ¿Y si el ataque fuera con una técnica nueva y más sofisticada que no haya experimentado anteriormente? ¿serían sus defensas capaces de resistir esta nueva y más potente clase de ataque?
- **Tercero, reaccione mejor.** En caso de un ataque cibernético, ¿cuál es el plan de la organización y cuál es su rol en él? ¿va a concentrarse en reparar rápidamente el daño o va a recopilar cuidadosamente las pruebas para optar por acciones legales? ¿cuál sería su primer paso?

Hay muchas cosas positivas. Hemos recorrido un largo camino en corto tiempo y estamos haciendo un buen trabajo, pero debemos hacerlo mejor, ya que nuestro enemigo viene con nuevas habilidades. En tal sentido, mientras que este informe, podría darle algo para trabajar en su organización, también debemos estar conectados para que podamos compartir y aprender de nuestras experiencias. Continuemos ayudándonos mutuamente.

Paul van Kessel

Líder Global de Seguridad Cibernética

La resiliencia cibernética

Las amenazas de todo tipo continúan evolucionando, y las organizaciones actuales encuentran que el panorama de amenazas cambia y presenta nuevos retos cada día. En respuesta, las organizaciones han aprendido a defenderse y responder mejor a lo largo de las décadas, pasando de medidas muy básicas y las clásicas respuestas *ad hoc*, a procesos sofisticados, robustos y formales. Eventos clave como el aumento en innovación digital, expansión de productos interconectados, la ley *Sarbanes-Oxley*, cambios regulatorios, crisis financieras, fallas catastróficas de productos, ataques terroristas y el crecimiento explosivo del crimen cibernético son sólo algunos ejemplos de porqué las organizaciones necesitan desarrollar sus capacidades defensivas y de protección. A continuación un breve resumen de esa evolución:

1970s	1980s	1990s	2000	2010
▸ Preparación para peligros naturales. ▸ Medidas de respuesta física, por ejemplo, evacuación y primeros auxilios. ▸ Requerimientos para asistencia externa.	▸ Dependencia en pocas nuevas tecnologías. ▸ Recuperación básica de desastres en respuesta a fallos de sistema. ▸ Desarrollo de antivirus. ▸ Administración de identidad y acceso.	▸ Inicio de la Gestión de riesgos empresariales. ▸ Cumplimiento normativo general. ▸ Enfoque en la continuidad de negocios.	▸ Avances en información y seguridad cibernética. ▸ Cambio a *on-line*. ▸ Gestión de terceros, por ejemplo, nube. ▸ Conectividad de dispositivos.	▸ *Shocks* globales (terrorismo, cambio climático, político). ▸ Resiliencia empresarial. ▸ Internet de las Cosas (*Internet of Things - IoT*). ▸ Infraestructura crítica. ▸ Espionaje y ataques cibernéticos patrocinados por estados.
Mainframes	**Cliente o Servidor**	**Internet**	***E-Commerce***	**Digital**

La resiliencia cibernética es un subgrupo de la resiliencia de negocio; se centra en qué tan resistente es una organización ante amenazas cibernéticas. Antes de entrar en detalles, veamos los tres componentes de alto nivel de la resiliencia cibernética y qué tan bien se están desempeñando - en general - las organizaciones en estas tres áreas:

Sentir

Sentir es la capacidad de las organizaciones para predecir y detectar las amenazas cibernéticas. Las organizaciones necesitan usar inteligencia cibernética y Defensa Activa para predecir qué amenazas o ataques se dirigen hacia ellas y detectarlos cuando lo hacen, antes de que el ataque sea exitoso. Necesitan saber qué va a suceder; y necesitan análisis sofisticados para obtener una advertencia temprana de la materialización de algún riesgo.

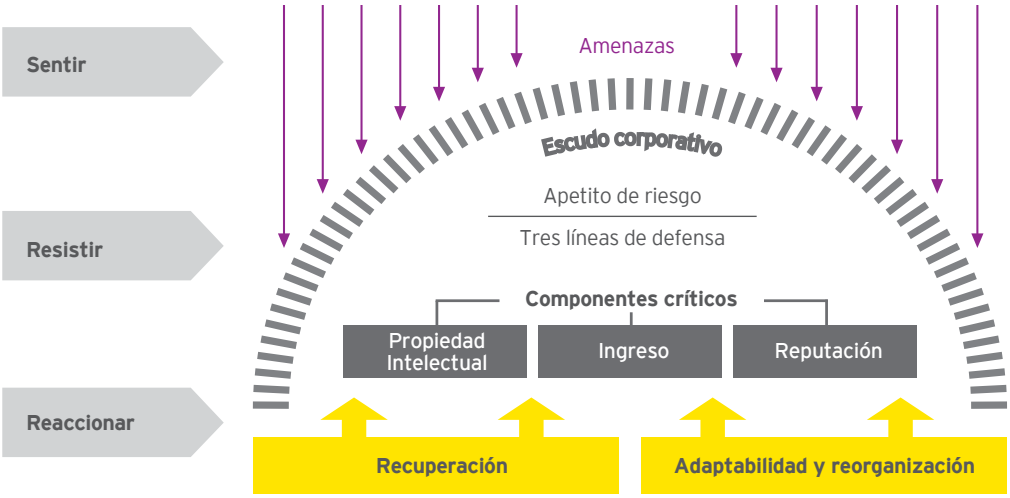
Resistir

Los mecanismos de resistencia son básicamente los escudos corporativos. Esto inicia con cuánto riesgo una organización está preparada para tomar a través de su ecosistema, seguido por el establecimiento de tres líneas de defensa:

1. Primera línea de defensa: Ejecutar medidas de control en las operaciones cotidianas.
2. Segunda línea de defensa: Despliegue de funciones de monitoreo tales como control interno, el departamento legal, gestión de riesgo y seguridad cibernética.
3. Tercera línea de defensa: El uso de un departamento de auditoría interna robusto.

Reaccionar

Si "Sentir" falla (la organización no detectó la amenaza que venía) y hay un desajuste en "Resistir" (las medidas de control no fueron lo suficientemente fuertes), las organizaciones deben estar listas para lidiar con la intrusión, con capacidades de respuesta y listas para gestionar la crisis. También necesitan estar preparadas para preservar la evidencia de la mejor manera posible para una posterior investigación de la intrusión, y poder satisfacer a las partes involucradas (clientes interesados, reguladores, inversionistas, fuerzas de seguridad y el público en general) quienes podrían presentar reclamos por pérdida o incumplimiento. Si los responsables son identificados, la organización podría iniciar una demanda contra ellos. Finalmente, las organizaciones deben estar preparadas para volver a operar como siempre en la forma más rápida posible, aprender de lo sucedido, y adaptar y remodelar la organización para mejorar su resiliencia cibernética.



El panorama general

Antes de explorar con más detalle, primero pintaremos un cuadro de la situación general de la resiliencia cibernética. A nivel alto, el mensaje es positivo: las organizaciones están avanzando en la dirección correcta. En los últimos años y bajo la presión de mayor regulación, las organizaciones han invertido en su escudo corporativo. Hay un progreso significativo en lo referente a la adopción de medidas para fortalecer este escudo y en los últimos dos a tres años, también hemos visto a organizaciones centrarse más en sus capacidades de "Sentir".

Sin embargo, la mayoría de las organizaciones se están quedando rezagadas respecto de la reacción ante una intrusión, ignorando la ya célebre frase: No es una cuestión de **si** vas a sufrir un ataque cibernético, es una cuestión de **cuándo** (y lo más probable es que **ya** hayas sufrido un ataque).

Hemos resumido el cuadro general, y en las siguientes secciones de este informe, exploraremos los componentes de la resiliencia cibernética con más detalle.

	Sentir (ver las amenazas que se aproximan)	**Resistir** (el escudo corporativo)	**Reaccionar** (recuperación ante una interrupción)
¿Dónde están las prioridades de las organizaciones?	Medio	Alto	Bajo
¿Dónde invierten las organizaciones?	Medio	Alto	Bajo
Compromiso de Directivos y *C-suite**	Bajo	Alto	Bajo
Calidad de reportes a Directorios	Bajo	Medio	Bajo

**C-suite: Top Senior Executives* (Ejecutivos de alto nivel)

¿Resiliencia cibernética o agilidad cibernética?

La gente que toma un vuelo en la actualidad, está impresionada por la rapidez con la que las aerolíneas han incorporado nuevas medidas de seguridad relacionadas con la carga de sus teléfonos móviles durante el vuelo. En el caso de la seguridad cibernética, existe un deseo similar. Las organizaciones desearían poder responder a los cambios lo más rápidamente posible. Normalmente se puede escuchar preguntas como ¿cómo puedo mejorar la respuesta de mi seguridad cibernética? y ¿cómo puedo responder rápidamente a lo que está sucediendo en el espacio cibernético?

Las organizaciones quieren saber cómo predecir la siguiente amenaza, y conocer los medios más utilizados para prevenirla. La inteligencia cibernética, gestión de amenazas cibernéticas y el software relacionado, consultoría e implementación de nuevas herramientas, se han convertido en prioridades en la mayoría de las organizaciones. Todo ello con la intención de mejorar nuestra agilidad cibernética, que es la capacidad de reaccionar a los cambios en el panorama de las amenazas.

Apuntar a alcanzar una mayor agilidad cibernética es fenomenal, y el dinero utilizado para tal fin está siendo bien invertido. Sin embargo, la pregunta principal que las organizaciones se deben hacer es: ¿son una organización cibernética resiliente? En otras palabras, ¿es su capacidad de seguridad cibernética lo suficientemente fuerte para mitigar todos los riesgos cibernéticos que enfrenta la empresa? Resiliencia cibernética no es sólo una cuestión de dar respuesta a las nuevas tecnologías y amenazas; si estas sólo se centran en respuestas, pueden dar lugar a medidas de seguridad *ad hoc* las cuales no crean una base estable, que es lo que se requiere para contar con una capacidad madura en seguridad cibernética.

Año tras año, nuestra **Encuesta Global de Seguridad de la Información** destaca los asuntos de seguridad cibernética más problemáticos y retadores para las empresas. En los últimos dos años, el 87% de los miembros del directorio y los ejecutivos de la *C-suite* han dicho que no confían en el nivel de seguridad cibernética de sus empresas. Así que todavía queda mucho por hacer. La atención a la agilidad cibernética es una necesidad - pero no nos dejemos persuadir y pensar que la agilidad cibernética es automáticamente la respuesta positiva a la pregunta de "¿somos cibernéticamente resilientes?"

87% Global

97% Perú

de los miembros del directorio y los C-suite han dicho que no confían en el nivel de seguridad cibernética de sus empresas.

Sentir

44%

Global

97%

Perú

no tienen SOC.

33%

Global

90%

Perú

no tienen un sistema de inteligencia contra amenazas.

¿Un alto nivel de confianza?

Las organizaciones han mejorado significativamente sus capacidades de "Sentir" en los últimos años. Muchas organizaciones están utilizando inteligencia cibernética para predecir lo que pueda ocurrir, instalando mecanismos de supervisión continua, como Centros Operativos de Seguridad (*Secure Operationg Centers - SOC*), identificando y gestionando vulnerabilidades, e instalando Defensas Activas: en general han adquirido mayor confianza en sus capacidades para predecir y detectar un ataque cibernético sofisticado. Este año, el 50% de las organizaciones consideran que es probable que sean capaces de hacerlo, el mayor nivel de confianza que hemos observado desde 2013.

Pero a pesar de estos puntos positivos, según nuestra encuesta, aún no son suficientes las organizaciones que están prestando atención a lo que hoy debe ser básico, y todos los días estas organizaciones están exponiendo a sus clientes, empleados, vendedores y, en última instancia su propio futuro, a un riesgo considerable. El hecho de que todavía hay trabajo por hacer, relacionado con las capacidades básicas de "Sentir", es confirmado por las siguientes conclusiones de la encuesta de este año:

- 44% no tienen *SOC*. En el Perú, es el 97% .
- 33% no tienen un programa de inteligencia contra amenazas. En el Perú, 90%.
- 55% no tienen, o sólo tienen una informal capacidad de identificación de vulnerabilidades. 97% en el Perú.

Además de estos fundamentos básicos, hay cuatro áreas específicas que necesitan una atención especial, y que podrían obligar a una organización a repensar lo que está haciendo.

Ha ocurrido una intrusión, pero parece que no hay daño

El 62% de las organizaciones encuestadas no aumentaría su inversión en seguridad cibernética después de experimentar una intrusión que pareciera no haber causado ningún daño; aunque en la mayoría de casos, sí hubo daño pero no se encontró evidencia inmediata que soporte esa afirmación.

Es común que los delincuentes cibernéticos realicen ataques de prueba antes de un gran ataque, ellos están al acecho después de una intromisión, o usan una intromisión como táctica de distracción para despistar a las organizaciones de sus objetivos reales. Las organizaciones deben saber que son vulneradas cada vez que reciben un ataque, y si no se ha encontrado evidencia del daño, deben considerar que es sólo cuestión de tiempo el encontrarla.

62%

Global

no aumentaría su inversión en seguridad cibernética luego de ser víctimas de intrusiones que aparentemente no causan daño.

Asegurar su ecosistema

En nuestro mundo digital e interconectado, los eventos en la red de proveedores, clientes, organismos gubernamentales (ecosistema), pueden seguir impactando a nuestra propia organización. Esta es un área de riesgo importante que a menudo se pasa por alto, como lo demuestran los siguientes hallazgos:

- 68% de los que respondieron, no incrementarían su inversión en seguridad de la información incluso si saben que uno de sus proveedores fue atacado y es una ruta directa de ataque a la organización.
- 58% no aumentaría su inversión si un competidor importante fuera atacado, aunque a los delincuentes cibernéticos les gusta atacar a organizaciones que son similares en infraestructura y marcos operativos, y utilizan lo aprendido en un ataque exitoso.

Un sistema sensor de una organización es mucho más efectivo cuando se tienen en cuenta también los eventos circundantes al ecosistema.

73%

Global

74%

Perú

están preocupados por el bajo nivel de conciencia sobre seguridad cibernética de los usuarios de dispositivos móviles.

49%

Global

90%

Perú

dudan de su capacidad para identificar tráfico sospechoso en sus redes.

El impacto del Internet de las Cosas (*IoT - Internet of Things*)

La aparición de *IoT* y la explosión en el número de dispositivos interconectados va a aumentar la presión sobre las capacidades de "Sentir" de una organización. Los siguientes son sólo algunos de los desafíos que esto crea para las organizaciones:

▸ **Desafíos relacionados con el número de dispositivos**

Las organizaciones están luchando con el enorme número de dispositivos que se convertirán en parte de sus redes en un período muy corto. Nuestros hallazgos muestran que el 73% de los encuestados, tanto a nivel global como en el Perú, están preocupados respecto a la falta de conciencia y el comportamiento de los usuarios de los dispositivos móviles. Otro gran grupo de organizaciones también están preocupadas por su capacidad de conocer todos sus activos (46%), cómo va a mantener estos dispositivos libres de virus o brechas de seguridad (43%), cómo poder parchar las vulnerabilidades lo suficientemente rápido (43%) y sobre su capacidad para gestionar el incremento de los puntos de acceso a su organización (35%).

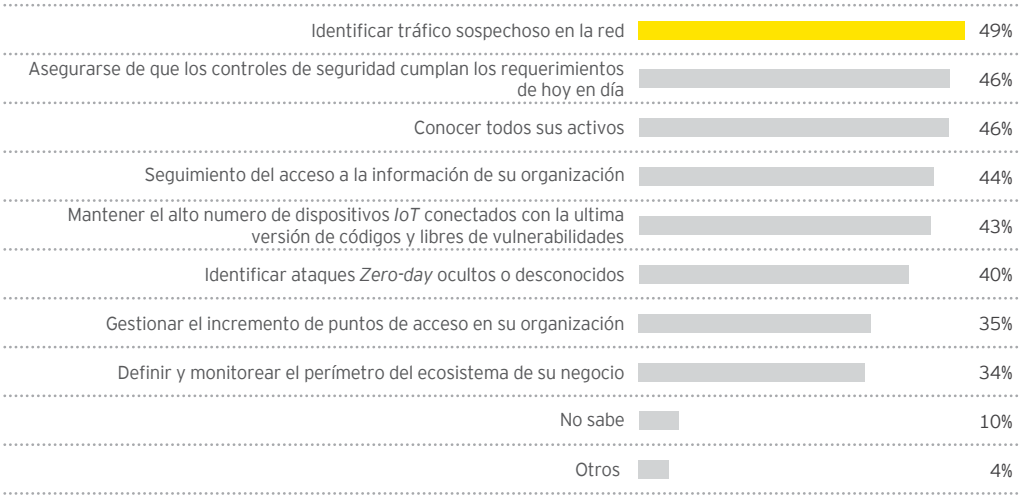
▸ **Retos relacionados con el tráfico de datos**

Las organizaciones no creen estar en la capacidad de identificar tráfico sospechoso en sus redes (49% a nivel global mientras que el Perú 90%), rastrear quién tiene acceso a sus datos (44%, similar a nuestro país en 52%) o ser capaces de identificar ataques ocultos y desconocidos del tipo *zero-day* (40% a nivel mundial y el en Perú 7%).

▸ **Los retos relacionados con el ecosistema**

El ecosistema va a crecer significativamente a medida que la conectividad con otras organizaciones se expanda, y aumente el volumen de datos que se intercambia entre ellas. Será cada vez más difícil identificar qué parte del ecosistema va a afectar a la organización y qué parte no, y será doblemente difícil si la propia seguridad cibernética de la organización se encuentra fragmentada. Como resultado, muchas organizaciones esperan tener dificultades en el monitoreo del perímetro de sus ecosistemas (34%).

¿Cuáles son los desafíos de seguridad de la información del *IoT* para su o rganización?



El intercambio de información y la colaboración están en aumento

Los gobiernos y otras entidades están cada vez más preocupados por su seguridad cibernética. El interés y el *momentum* de regulaciones específicas de industrias relacionadas a los riesgos cibernéticos están aumentando; por lo tanto, debemos esperar la aparición de nuevas regulaciones y leyes. En muchas partes del mundo, se están desarrollando estándares de organizaciones de infraestructura crítica, y hay una necesidad real a un mayor intercambio de información y una mayor colaboración, así como la notificación obligatoria de ataques cibernéticos, para que el crimen cibernético pueda combatirse en conjunto.

Cabe prever que esto se convertirá en una medida obligatoria, e incluso, si no sucede en el corto plazo, el entorno de hoy en día hará que los reguladores, partes interesadas, socios de negocios e incluso los clientes, deseen saber más sobre su seguridad cibernética.

Así que esté preparado para informar y buscar oportunidades para compartir y colaborar hoy. Actualmente nuestra encuesta reveló lo siguiente:

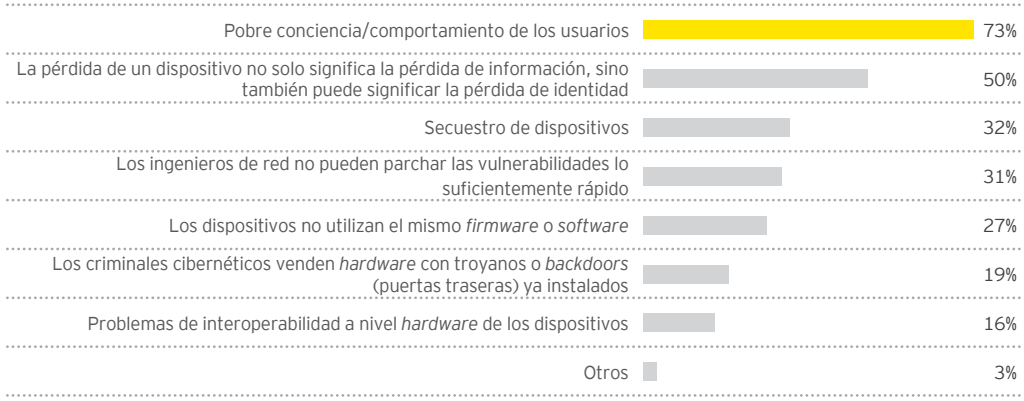
- 49% de los *SOCs* de nuestros encuestados colaboran y comparten datos con otros actores de la misma industria.
- 38% de los *SOCs* de nuestros encuestados colaboran y comparten datos con otros *SOCs* públicos.

49%

Global

de los SOCs encuestados respondieron que colaboran y comparten data con otros actores de la misma industria.

¿Cuáles son los principales riesgos asociados con el creciente uso de dispositivos móviles (por ejemplo, portátiles, *tablets*, *smartphones*) para su organización?



Los criminales cibernéticos pueden ser despiadados, y su comportamiento y métodos son casi imposibles de predecir.

Los criminales cibernéticos - como otras organizaciones criminales - están preparados para comportarse de forma que la mayoría de nosotros no pueda comprender. Sus acciones transmiten un conjunto diferente de valores, ética y moralidad, y a menudo son impulsados por motivaciones que son difíciles de sondear. A parte del fraude y robo más habitual y esperado, los consumidores temen cada vez más que los automóviles sean *hackeados* para causar accidentes, y algunas organizaciones de infraestructura crítica están viendo el riesgo de secuestro y rescate cibernético ya como una realidad. Tal es la creatividad de las redes criminales que siempre encontrarán nuevas maneras de lanzar ataques para beneficio personal, o para lograr titulares en prensa por alguna causa. Sentir, Resistir y Reaccionar juegan una parte fundamentalmente importante en la protección del ecosistema cibernético, especialmente con el crecimiento del *IoT*. Sin seguridad cibernética eficaz muchas organizaciones y gobiernos no sólo están arriesgando sus datos y la propiedad intelectual, también pueden estar poniendo a individuos en riesgo, y en el futuro, podríamos esperar aún más daño colateral.

Resistir

Enfocarse en riesgos cibernéticos, no solamente en seguridad cibernética

86%

Global

90%

Perú

dijo que su función de seguridad cibernética no satisface plenamente las necesidades de su organización.

En general, las organizaciones han mejorado considerablemente sus habilidades para resistir ataques, y muchas de ellas pueden decir que se están defendiendo con éxito de miles de ataques cada día. Pero los ataques toman formas diferentes y son cada vez más complejos, y el ejecutar las medidas de control en el escudo corporativo puede funcionar en contra de ataques simples como Negación de Servicio o Virus Informático, pero no funciona tan bien contra el ataque sofisticado y persistente que los delincuentes cibernéticos dedicados y organizados están lanzando contra sus objetivos todos los días.

- El año pasado, el 88% de los encuestados dijo que su función de seguridad cibernética no satisface plenamente las necesidades de su organización. Este año, el 86% de encuestados lo reafirmó, lo que no representa una mejora significativa. A pesar de los pasos que han tomado las organizaciones, todavía no es suficiente para hacer frente a esta situación.

Centrarse en los riesgos cibernéticos, no sólo en la seguridad cibernética

En esta encuesta, casi la mitad de los encuestados (48%) dicen que sus controles de seguridad desactualizados son un área de alta vulnerabilidad, lo cual es consistente con los resultados de nuestras encuestas a partir del 2013 y 2014, mientras que en el 2015 sólo el 34% calificó esto como un área de alta vulnerabilidad. En general, en el 2015 se produjo un aumento significativo de la confianza respecto de las vulnerabilidades y amenazas, considerándolas como un desafío menor a los años anteriores. Esa confianza, basada en el hecho de ser capaz de resistir los ataques, ha sido de corta duración ante el crecimiento de riesgos y amenazas relacionadas a los empleados, y el mayor conocimiento de cómo los carteles criminales están apuntando específicamente a esta debilidad humana. Este año se registra un importante aumento de la calificación de su exposición al riesgo. En el 2015, las organizaciones pensaban que habían empezado a resolver el problema de la seguridad cibernética y eran más capaces de resistir los ataques, solamente para darse cuenta luego que habían sido vulneradas, o para simplemente hacerse más conscientes de las amenazas.

¿Qué amenazas y vulnerabilidades han aumentado más su riesgo en los últimos 12 meses?

El gráfico muestra una cifra porcentual total para los ítems clasificados 1 (más alto) y 2 (alto), desde 2013-16.

	2013	2014	2015	2016
Vulnerabilidades				
Empleados descuidados o desinformados	53%	57%	44%	55%
Controles de seguridad o arquitectura de información desactualizados	51%	52%	34%	48%
Acceso no autorizado	34%	34%	32%	54%
Amenazas				
Malware	41%	34%	43%	52%
Suplantación de identidad (*Phishing*)	39%	39%	44%	51%
Ataques cibernéticos para robar información financiera	46%	51%	33%	45%
Ataques cibernéticos para robar *IPs* o datos	41%	44%	30%	42%
Ataque internos	28%	31%	27%	33%

57%

Global

10%

Perú

ha tenido un incidente significativo de seguridad cibernética recientemente.

¿Dónde deben centrarse las organizaciones para resistir mejor los ataques de hoy?

Activar sus defensas

Si bien la naturaleza de los ataques ha cambiado, resistir, defender, mitigar y neutralizar ataques han sido durante mucho tiempo el núcleo necesario de la seguridad cibernética. Los servicios y herramientas que una organización puede usar para resistir, han mantenido el ritmo, y muchas soluciones están disponibles hoy en día. Sin embargo, nuestra encuesta revela que el 57% de los encuestados ha tenido un incidente significativo de seguridad cibernética recientemente, lo que demuestra que todavía hay más trabajo para hacer para fortalecer el escudo corporativo. Los niveles de madurez son todavía demasiado bajos en muchas áreas críticas, y mejorarlos sería un importante paso adelante para cualquier organización.

El porcentaje de encuestados que clasificarían como maduro este proceso de gestión de seguridad de la información:

- Seguridad del *software*: 29%
- Seguimiento de seguridad: 38%
- Gestión de incidentes: 38%
- Gestión de identidades y accesos: 38%
- Seguridad de red: 52%

Tome un enfoque poco ortodoxo

La capacidad de resistencia requiere un enfoque multifacético. Las defensas se suelen considerar como barreras difíciles, como el cifrado o *firewalls* que detienen y/o neutralizan un ataque; pero hay otras formas en que las organizaciones pueden minimizar el impacto de un ataque y ayudar a la organización a resistir.

- **Cambio de un sistema de seguridad a prueba de fallos a uno de seguro en fallos**

  Las organizaciones han acertado al enfocarse hasta ahora en la construcción de operaciones robustas, resistentes y resilientes a prueba de fallas que pueden soportar ataques cibernéticos repentinos. Pero en la coyuntura actual de ataques impredecibles

y sin precedentes, un enfoque de seguridad a prueba de fallas no puede ser la única opción. El nuevo objetivo debe ser diseñar un sistema que sea seguro al fallar. La seguridad cibernética debe ser más inteligente y más fuerte, con un enfoque de resiliencia blanda. Esto significa que al detectar una amenaza, haya mecanismos diseñados para absorber el ataque, reducir la velocidad y el impacto de este, así como aceptar la posibilidad de una falla parcial del sistema como una forma de limitar el daño a la totalidad.

▸ **De la protección al sacrificio**

Las tecnologías actuales permiten sacrificar porciones de información u operaciones en el interés de proteger la red en su totalidad. Si está correctamente configurado en el marco del apetito al riesgo de la organización, esto puede ser llevado a cabo como una respuesta automatizada. Cuando el *SOC* reconoce una amenaza de alto nivel para el sistema, el propietario del sistema recibe una alerta y el sistema es cerrado para evitar la propagación de la amenaza.

Cada año los presupuestos aumentan, pero ¿es suficiente?

Entre el 2013 y el 2016 hemos visto ciertos incrementos en los presupuestos, con un 53% de los encuestados este año diciendo que sus presupuestos aumentaron en los últimos 12 meses, en comparación con el 43% en 2013, y el 55% de los encuestados hoy en día afirmando que sus presupuestos aumentarán en los próximos 12 meses, en comparación con el 50% en el 2013. Las cantidades que se invierten también están aumentando. En el 2013, el 76% de los encuestados estaba gastando menos de US$ 2 millones en total (que incluía personas, procesos y tecnología); hoy en día sólo el 64% está gastando menos de 2 millones de dólares y ha habido un aumento en el número de organizaciones que gastan entre 10 millones y 50 millones de dólares.

Sin embargo, las organizaciones dicen que se necesita más financiamiento, el 61% citando las limitaciones presupuestarias como un desafío y el 69% de los encuestados diciendo que necesitan hasta un 50% más de presupuesto. Y no es sólo presupuesto lo que se necesita. Mientras que el presupuesto adicional puede ayudar a aliviar la escasez de habilidades, el dinero no puede comprar el apoyo ejecutivo que también es muy necesario.

53%

Global

81%

Perú

dicen que sus presupuestos aumentaron en los últimos 12 meses.

86%

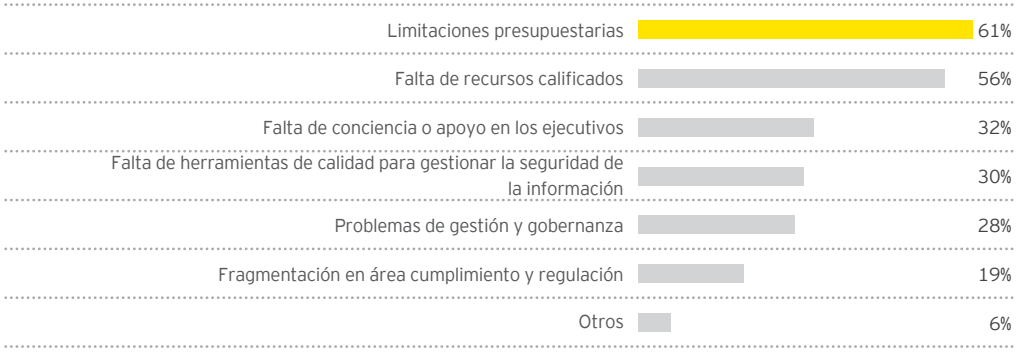
Global

42%

Perú

dicen que necesitan hasta un 50% más de capital.

¿Cuáles son los principales obstáculos o razones que enfrentan la contribución y el valor de la operación de seguridad de la información en las organizaciones?



El papel de los líderes

El liderazgo ejecutivo y el apoyo son fundamentales para alcanzar una resiliencia cibernética efectiva. A diferencia de las actividades de Sentir y Resistir tradicionales que pueden ser vistas como el dominio del *CIO*, la resiliencia cibernética requiere que los altos ejecutivos participen activamente y lideren la fase de Reacción. Desde el 2013, el estudio ha informado que el 31% -32% de los encuestados indican que hay una falta de conciencia y apoyo de la alta gerencia, lo cual dificulta lograr eficacia en las medidas de seguridad cibernética. Esta consistencia año tras año sugiere que no se está haciendo lo suficiente para resolver esta situación, o los intentos han llegado a un punto muerto y el mensaje no cala en nuestra *C-suite*.

La importancia de informar

Entre nuestros encuestados, el 75% menciona que los responsables de la seguridad de la información no tienen un lugar en los comités o directorios, por lo que en estas reuniones se tiene que confiar en los reportes que se brindan con información relacionada. Nuestra encuesta reveló lo siguiente:

- Sólo el 25% de los reportes brindan una visión general de las amenazas.
- Sólo el 35% de los reportes muestran dónde se necesitaron mejoras en la seguridad de la información de la organización.
- 89% de las organizaciones no evalúan el impacto a nivel financiero de cada intrusión significativa, y de aquellos que han sido víctimas de uno efectivamente durante este año, casi la mitad (49%) no tienen idea de cuál es o cuál podría ser el daño financiero.

Con una tan baja calidad de los reportes, no es de extrañar que el 52% de los encuestados piensen que su alta gerencia o directores no conocen bien los riesgos que la organización está tomando y las medidas que están en marcha. En otras palabras, nuestra encuesta sugiere que cerca de la mitad de las juntas directivas no tienen una idea clara de la mayor amenaza para sus organizaciones hoy en día.

89%

Global

90%

Perú

de las organizaciones no evalúan el impacto a nivel financiero de cada intrusión significativa.

49%

Global

22%

Perú

no tienen idea de cual es o cual podría ser el daño financiero.

Reaccionar

Los servicios de emergencia de hoy: programa de respuesta a intrusiones cibernéticas

Dada la probabilidad de que todas las empresas enfrenten eventualmente una intrusión cibernética, es fundamental que las empresas desarrollen un esquema de respuesta fuerte y centralizada como parte de su estrategia global de gestión de riesgos.

Un programa cibernético de respuesta a intrusiones cibernéticas centralizado (*Cyber Breach Response Program - CBRP* por sus siglas en inglés) es el punto focal que reúne a las partes interesadas que deben colaborar para resolver una intrusión. El *CBRP* debe estar dirigido por alguien con experiencia en tecnología y capaz de manejar la respuesta operativa y táctica cotidiana, además de que debe estar equipado con una profunda experiencia legal y de cumplimiento, ya que estos eventos pueden desencadenar complejas cuestiones legales y regulatorias con impacto en los estados financieros.

El *CBRP* va más allá de la capacidad de una oficina tradicional de gestión de programación. En su función de coordinación y supervisión, el *CBRP* puede ayudar a asegurar que el plan de continuidad de negocios de una organización se implemente apropiadamente, que se desarrolle y se aplique un plan de comunicación entre todos los interesados internos y que todos los grupos se gestionen de forma centralizada. En resumen, el *CBRP* proporciona orientación a todas las líneas de negocio involucradas en la respuesta. El programa establece un nivel de comprensión sobre qué información crítica debe ser conocida por los líderes senior, así como cuándo y cómo expresarla, lo que permite una reacción continua con precisión y velocidad, mientras una probable intrusión ocurra, desarrollándose durante días, semanas o incluso meses.

Un *CBRP* efectivo debe incluir a los grupos clave en una intrusión de alto impacto. Aun cuando los investigadores necesiten trabajar estrechamente con el área de seguridad de la información y el personal de TI para determinar el vector de ataque, las redes y sistemas vulnerados y el alcance de los activos robados o afectados, un *CBRP* debe ser el eje de respuesta. El *CBRP* ayuda a no sólo supervisar el proceso de identificación, recopilación y preservación de las pruebas, el análisis forense de datos y la evaluación de impacto, sino que también puede dirigir y modificar la investigación basada en el análisis de los patrones de hechos ocurridos.

El *CBRP* ayuda a asegurar un flujo fluido y oportuno de información entre las partes interesadas internas y ayuda a la organización a gestionar las, a veces complejas, relaciones con abogados externos, y entes reguladores. Un *CBRP* robusto, por lo tanto, permite una respuesta rentable que mitiga los impactos de una intrusión integrando a las partes interesadas.

57%

Global

53%

Perú

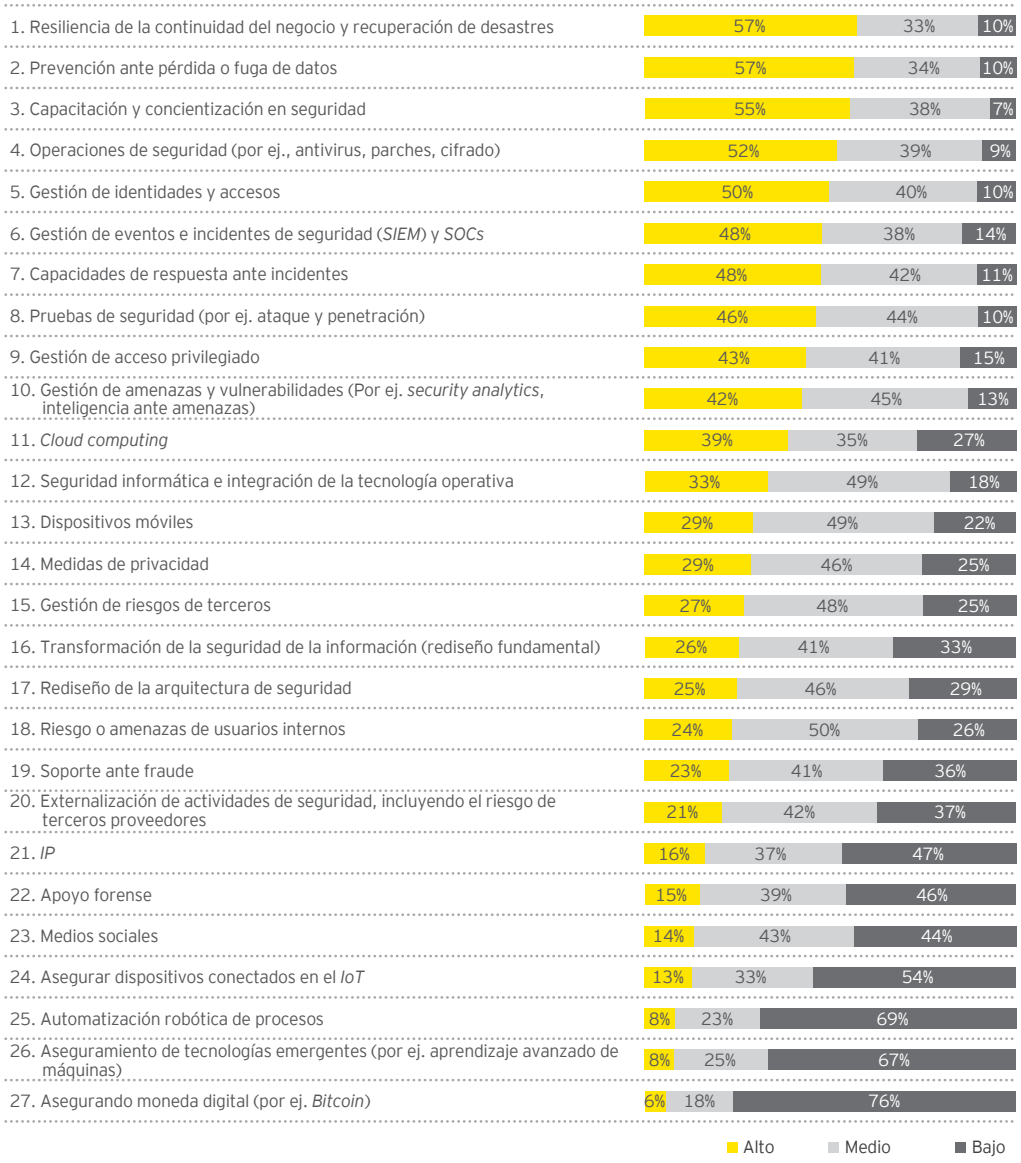
de las organizaciones calificó la BCM como su principal prioridad, junto con prevención ante pérdidas o fuga de datos.

¿Cuáles son las prioridades de Reaccionar?

La gestión de la continuidad de negocio (*Business Continuity Management - BCM* por sus siglas en inglés) ha sido la principal habilidad de una organización para reaccionar ante una amenaza, ataque u otra interrupción en sus operaciones durante muchos años. Como área clave de la seguridad cibernética, esta ha ocupado el número 1 o 2 de alta prioridad en nuestra encuesta desde 2013, por lo que es entendible la importancia de tener algunas de estas habilidades como parte de Reaccionar. Una vez más, este año el 57% de las organizaciones calificaron al *BCM* como una prioridad conjuntamente con la prevención ante pérdida o fuga de datos.

Seguridad de la información y la gestión de eventos (*Security Information and Event Management - SIEM* por sus siglas en inglés), junto con los centros de operaciones de seguridad (*SOC* por sus siglas en inglés), ocupan el sexto lugar, con un 46% de los encuestados diciendo que van a gastar más en estas dos áreas en los próximos 12 meses, luego de conciencia de seguridad y entrenamiento.

¿Cuál de las siguientes áreas de seguridad de la información definiría como prioridades altas, medianas o bajas para su organización en los próximos 12 meses?



¿En qué se gasta el dinero?

En qué gastan las organizaciones sus presupuestos es ya un escenario diferente. Al revisar la lista de donde las organizaciones quieren gastar más, *BCM* ocupa el noveno lugar. Las organizaciones pueden sentir que *BCM* ha sido bien financiado en el pasado y ahora están invirtiendo en otras capacidades de Reaccionar.

En comparación con el año anterior, ¿su organización planea gastar más, menos o relativamente la misma cantidad durante el próximo año para las siguientes actividades?

No hay mucha intención de invertir en otras capacidades de adaptación y rediseño:

- **Adaptarse:** Al mirar el horizonte de las amenazas y los actores relacionados, la organización resiliente necesita ser flexible y ágil para adaptar sus procesos de negocio y mecanismos de protección.
- **Rediseño:** Se trata de la reingeniería necesaria para mejorar los mecanismos flexibles y operativos para una organización cada vez más segura y sostenible.

A pesar de que los controles de seguridad de la información o arquitectura obsoleta son la segunda vulnerabilidad más alta, el 74% dice que una transformación de seguridad de la información es una prioridad media o baja y el 75% dice que el rediseño de la arquitectura de seguridad es de prioridad media o baja.

42%

Global

35%

Perú

no cuenta con una estrategia o plan de comunicación en caso de un ataque significativo.

39%

Global

95%

Perú

afirma que emitirían un comunicado público.

Al reaccionar ante un ataque, el directorio debe mostrar liderazgo

Cuando se trata de atender de inmediato un ataque cibernético que ha dañado a la organización, no hay hoy en día nada que la junta pueda ocultar. Si alguna debilidad o fracaso en los planes de recuperación se materializó, y mientras más tiempo estos problemas continúen, peor será la situación. Algunas organizaciones pueden recuperarse físicamente de un ataque, pero su reputación y confianza pueden ser destruidas. La clave es coordinar y dirigir las comunicaciones antes de que la fuerza de los medios de comunicación tradicionales y los medios de comunicación social se hagan cargo.

Hay muchas organizaciones que aún no están preparadas:

- 42% no cuenta con una estrategia o plan de comunicación en caso de un ataque significativo.
- Durante los primeros siete días después de un ataque:
  - 39% dice que emitirían un comunicado público.
  - 70% notificaría a organismos reguladores y entidades de cumplimiento.
  - 46% no notificaría a los clientes, incluso cuando se haya comprometido su información.
  - 56% no notificaría a los proveedores, incluso cuando hayan comprometido sus datos.

Qué, cómo y cuándo comunicar pueden presentar desafíos significativos

- Hoy en día, muchas de las regulaciones sobre la notificación de ataques cibernéticos dicen que se debe notificar a los clientes dentro de cierto número de días - 60 días, por ejemplo.* El problema es que muchos ataques cibernéticos no se descubren durante meses y a veces años. Y en los casos en que la aplicación de la ley está involucrada, es posible que se solicite no notificar a los clientes mientras las investigaciones estén en curso.
- Los clientes pueden tener derecho, o sentir que tienen derecho a ser recompensados ante el posible filtraje de su información. Por ejemplo en los EE.UU., se está discutiendo que un cliente reciba un seguro gratuito por un año ante el posible robo de identidad. Es claro que no todas las intrusiones crean una situación donde un cliente necesitaría algo por el estilo, pero este tipo de compensaciones podrían aumentar los costos sin proporcionar un beneficio real para el cliente, y podría ser perjudicial para la marca y su reputación.
- Por último, existe una creciente idea de que puede ser perjudicial el notificar a los clientes cada vez que hay una intrusión, especialmente si el riesgo es bajo, ya que pueden volverse insensibles ante estos hechos y no responder cuando ocurre un incidente grave o más dañino. Si pensamos en los últimos dos años, no es improbable que la misma persona haya sido informada sobre un ataque a su proveedor de telefonía móvil, al proveedor en línea que usa, a su proveedor de correo electrónico y que se les hayan avisado que posiblemente los datos de su tarjeta de crédito hayan sido vendidos y que sus registros de seguro social estén en manos de criminales, y no hay nada que puedan hacer al respecto. Es demasiada información y la gente empezará a ignorarla.

* Como en el caso de la hoja de ruta de la *NAIC* para la Protección al Consumidor en seguridad cibernética en los EE.UU (*National Association of Insurance Commissioners – NAIC* por sus siglas en inglés).

5%

Global

ha realizado recientemente cambios significativos a la estrategia y planes de su empresa.

79%

Global

ejecuta su propio phishing.

Liderar la recuperación de la organización

Para que el *CIO* pueda apoyar al negocio durante la fase de adaptación y reestructuración, necesita comprender completamente la dirección estratégica, el apetito de riesgo y las operaciones de la organización. Al reunir a los estrategas corporativos y al equipo de seguridad corporativa, se puede alinear la solución de seguridad cibernética y la estrategia general de la organización. Sin embargo, nuestra encuesta muestra que no existe una buena conexión entre la función de seguridad cibernética y la estrategia y planificación de la organización.

- Sólo el 5% de los encuestados ha realizado recientemente un cambio en la estrategia y planes de la organización, después de identificar que estaban expuestos a un riesgo excesivo.
- Sólo el 22% afirma que ha considerado las implicancias de seguridad de las actuales estrategias y planes de su organización.

Hacer preguntas más difíciles y cerrar las brechas

Nuestra encuesta reveló que las organizaciones prefieren confiar en sí mismas para probar o gestionar su propia seguridad cibernética. En la fase de recuperación, quizás valga la pena considerar si esta práctica deba continuar. En la actualidad se cumplen los siguientes hechos:

- 79% ejecuta su propio *phishing*.
- 64% ejecuta sus propias pruebas de penetración.
- 81% hace su propia investigación de incidentes.
- 83% hace su propio análisis de inteligencia de amenazas.

Nuestra encuesta también encontró brechas que necesitan ser abordadas. A pesar de tener empleados descuidados, *phishing* y *malware* como amenazas importantes y conocidas, sólo un 24% tiene un plan de respuesta a incidentes que les ayudaría a recuperarse del malware y el mal comportamiento de los empleados.

En general, aún se necesitan mejoras considerables

Aunque las capacidades de Reacción se desempeñan bien en las clasificaciones de prioridad, el dinero invertido en esta área es aún relativamente bajo. Se puso de manifiesto - a partir del estado general de la resiliencia cibernética (sección 1) - que Reacción es el área donde la mayor parte del trabajo todavía está por hacerse. Cuanto sea más claro que el escudo corporativo no puede resistir a todas las amenazas, más atención recibirá la capacidad de Reacción.

81%

Global

97%

Perú

ejecuta su propia investigación de incidentes.

Características clave de una empresa con resiliencia cibernética

Entiende el negocio

La resiliencia cibernética exige una respuesta de toda la organización. Comienza con una comprensión profunda de los negocios y el panorama operativo, para saber qué flujo de trabajo debe ser preservado para que la organización pueda seguir operando y salvaguardar a las personas, los activos y el valor general de la marca, a pesar de un ataque cibernético.

Entiende el ecosistema cibernético

Mapea y evalúa las relaciones que la organización tiene a través del ecosistema cibernético e identifica qué riesgos existen. Realiza una evaluación del riesgo de la presencia cibernética de la organización en el ecosistema, determinando aquellos factores que afectan el alcance del control que la organización tiene sobre su ecosistema.

Determina los activos críticos - las joyas de la corona

La mayoría de las organizaciones sobreprotege algunos activos y desprotege otros. En nuestra encuesta:

- El 51% clasificó la información personal identificable del cliente como la información número 1 o número 2 más valiosa para los criminales cibernéticos en la organización.
- Sólo el 11% ha catalogado su *IP* patentada (*Intellectual Property – IP* por sus siglas en inglés) como información vulnerable número 1 o número 2.
- Se consideró que la información personal de los ejecutivos o miembros de directorio era más valiosa que la información sobre *R&D* (Investigación y Desarrollo), la propiedad intelectual patentada y la propiedad intelectual no patentada y, en general, equivalente a los planes estratégicos corporativos.

Determina los factores de riesgo

Las funciones de seguridad cibernética sólo pueden lograr un éxito limitado con una visión limitada del panorama de riesgo y amenaza. Por encima de todas las tecnologías y herramientas que pueden proporcionar una mejor conciencia, inteligencia e identificación de amenazas, se encuentra el concepto de colaboración. El compartir información sobre el riesgo y el panorama de amenazas de todas las funciones de negocio permite a la organización entender mejor su panorama de riesgo y exponer las brechas de seguridad. Este intercambio y colaboración puede extenderse a otras organizaciones (socios, proveedores) en el mismo ecosistema.

Entonces, las organizaciones necesitan preguntarse lo siguiente:

- ¿Cuánto podemos hacer para manejar cualquier riesgo residual?
- ¿Estamos preparados para aceptar cierto nivel de riesgo?
- ¿Qué podemos intentar controlar y qué debemos aceptar como fuera de nuestro control?

Gestiona el elemento humano con liderazgo excepcional

Después de un ataque cibernético, como en cualquier situación caótica, las personas necesitan estar preparadas y entrenadas sobre cómo responder y comportarse. Con apoyo tecnológico en toda la organización, cada empleado debe estar bien informado. Es esencial la comunicación, la dirección y el establecimiento de un liderazgo claro; así como roles o tareas claramente definidos que se puedan ejecutar para ayudar a la organización a volver a operar.

Crea una cultura preparada para el cambio

La capacidad de reaccionar rápidamente a un ataque cibernético minimizará la posibilidad de impactos materiales a largo plazo. Las organizaciones que desarrollan capacidades de respuesta superiores, integradas y automatizadas pueden activar el liderazgo no rutinario, la gestión de crisis y la coordinación de los recursos de toda la empresa. Como ejercicio de simulación, las organizaciones pueden probar la gestión de crisis existente, sus actuales prácticas y los riesgos para asegurarse de que están totalmente alineados con la estrategia empresarial de la organización y con su nivel de apetito por el riesgo.

Las organizaciones también deben desarrollar e implementar juegos de guerra hechos a medida que incluyan una revisión de cualquier centro de mando y control, manuales y planes de resiliencia cibernética.

Realiza investigaciones formales y se prepara para enjuiciamiento

Para proteger los intereses de la organización en caso de una intrusión cibernética a gran escala, el *CIO* debe estar preparado para trabajar con los altos ejecutivos de seguridad, asesores jurídicos y asesores externos. Juntos, ellos:

- Reunirán la evidencia forense, para respaldar una investigación más profunda.
- Determinarán si los atacantes aún se mantienen en las redes y sistemas de la organización, y si los programas maliciosos o de *malware* pueden volver a sabotear la organización en el futuro.
- Efectuarán una investigación más profunda sobre los sujetos que realizaron el ataque, cómo lo realizaron, para quién y porqué.
- Serán capaces de presentar una demanda y/o enjuiciamiento criminal contra el atacante, así como aquellos que ayudaron e incitaron al atacante. También se pueden presentar demandas contra proveedores de productos y servicios que no cumplieron con las obligaciones contractuales de construir, operar, probar o mantener la seguridad cibernética.

Metodología de la encuesta

La 19º **Encuesta Global de Seguridad de la Información de EY** recoge las respuestas de 1,735 líderes de la *C-suite* y ejecutivos de seguridad de la información y TI que representan a muchas de las compañías globales más grandes y reconocidas del mundo. La investigación se llevó a cabo entre junio y agosto de 2016.

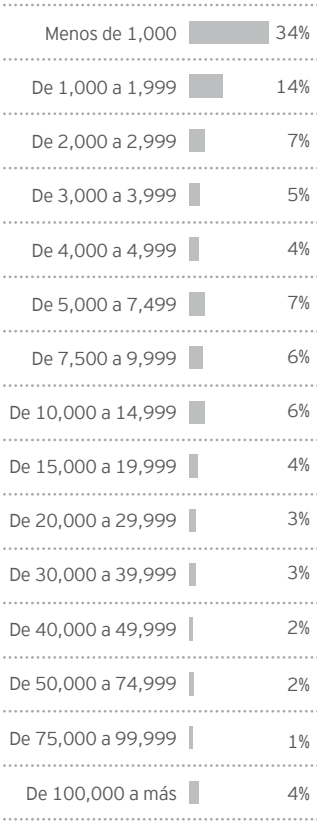
Encuestados por posición

Gerente de Seguridad de la Información	23%
Ejecutivo de Seguridad de la Información	12%
Gerente de Informática	12%
Ejecutivo de Informática	11%
Gerente de Seguridad	3%
Director/administrador de Auditoría Interna	3%
Gerente de Tecnología	3%
Administrador de Redes / Sistemas	2%
Ejecutivo de unidad de negocio / Vicepresidente	2%
Gerente de Finanzas	1%
Gerente de Riesgos	1%
Otros	27%

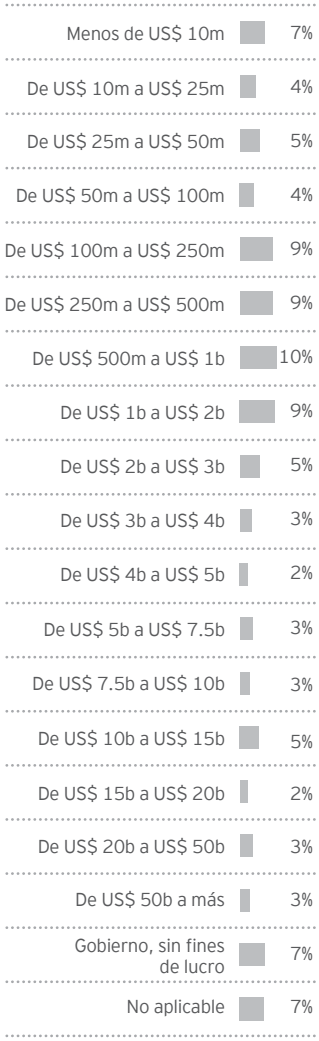
Encuestados por área

Europa, Medio Oriente, India y África	38%
Américas	38%
Asia-Pacífico y Japón	24%

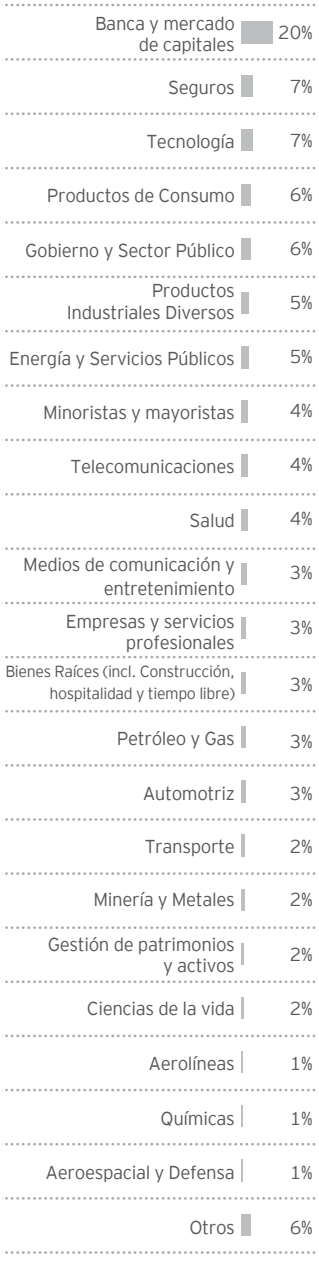
Encuestados por número de empleados



Encuestados por ingresos anuales totales de la empresa



Encuestados por sector de la industria



II.

¿Cómo encontrar a los criminales antes que cometan un delito cibernético?

Introducción

Inteligencia de amenazas cibernéticas

El mercado ofrece muchas descripciones diferentes de la inteligencia de las amenazas cibernéticas (*Cyber Threat Intelligence - CTI* por sus siglas en inglés), y la mayoría forma parte de diferentes tipos de fuentes de información que no están necesariamente alineadas con ninguna organización o industria en particular. Esencialmente, cualquier tipo de inteligencia de amenazas es simplemente la información evaluada, y sólo puede entenderse en el contexto en el que se crea y el propósito propuesto para su uso. El objetivo suele ser el tener un entendimiento del riesgo para que sea considerado por la gerencia, ya sea en un nivel operacional, táctico o estratégico.

Por lo tanto, es necesario que las organizaciones entiendan cómo la inteligencia de amenazas puede aumentar su comprensión de las situaciones relevantes y a qué decisiones puede contribuir.

Sin esta línea de pensamiento y una formulación del propósito, las organizaciones no sabrán qué preguntas hacer sobre toda la información disponible (ya sea de origen interno o externo) para refinar la recopilación de información y ayudar a dirigir el análisis, ni cómo incorporar la inteligencia en los procesos de toma de decisiones. Para la seguridad cibernética, gran parte de este pensamiento y priorización se incorpora en los sistemas que están programados para recopilar y monitorear la información, pero el componente de análisis humano sigue siendo crucial.

En general, las organizaciones aún no entienden completamente qué preguntar sobre *CTI* ni cómo entender los diferentes niveles e implicancias. Para funciones más operativas, por ejemplo, las asociadas con un centro de operaciones de seguridad (*SOC* por sus siglas en inglés), *CTI* será muy técnico y estará estrechamente relacionado con la información de vulnerabilidad; mientras que para el *CEO*, inteligencia de amenazas cibernéticas puede equiparar exclusivamente a los titulares o informes que reciben en varios eventos cibernéticos, lo que puede no ayudarles a entender cómo podrían ser relevantes para su organización.

Desde el punto de vista de EY, esta falta de comprensión y/o la limitada aplicación actualmente asociada con *CTI* significa que muchas organizaciones están perdiendo una de las oportunidades más poderosas de la era digital: la oportunidad de adelantarse al criminal cibernético.

27%

Perú

dicen que es poco probable que puedan detectar un ataque sofisticado.

Un programa de *CTI* robusto puede arrojar luz sobre una multitud de negocios estratégicos y riesgos, mientras que proporciona acciones altamente técnicas, contramedidas y métricas para el programa de seguridad cibernética en general. Puede potencialmente proporcionar respuestas a preguntas como:

- ¿Cuáles son las amenazas más importantes que enfrenta nuestra organización?
- ¿Qué activos (potencialmente) están siendo amenazados y por quién?
- ¿Cómo puede nuestra organización protegerse contra estas amenazas cibernéticas?
- ¿Cómo puede nuestra organización utilizar la inteligencia para aumentar y mejorar nuestra seguridad y las operaciones comerciales?

Mediante la creación de un programa *CTI*, las organizaciones son capaces de madurar simultáneamente los procesos de seguridad cibernética existentes y desarrollar una visión general de su paisaje específico de amenazas.

¿Qué significa la Inteligencia de amenazas cibernéticas?

64%

Global

no cuenta con un programa de inteligencia de amenazas.

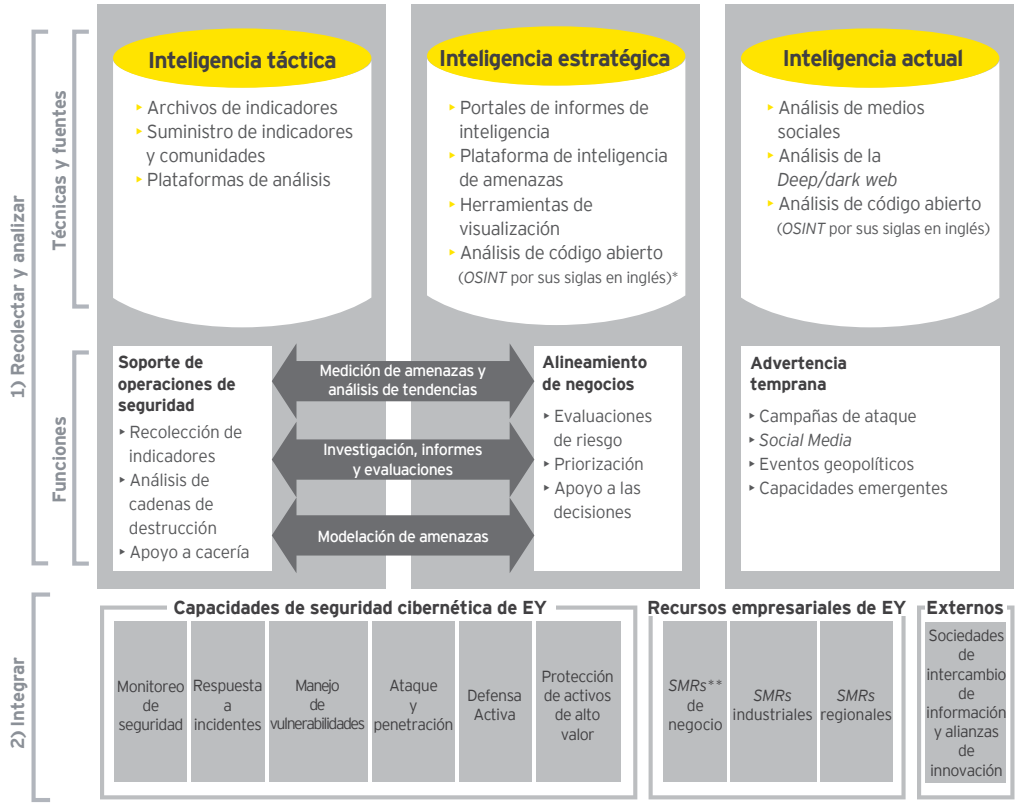
***CTI* es un proceso avanzado que permite a la organización reunir ideas valiosas basadas en el análisis de los riesgos contextuales y situacionales y puede adaptarse al paisaje de amenazas específico de la organización, su industria y mercados.**

El proceso gestiona la recopilación, el análisis, la integración y la producción de información previamente desunida con el fin de extraer información holística y basada en evidencias sobre el paisaje de amenazas único de una organización. Esta inteligencia puede hacer una diferencia significativa en la capacidad de la organización para anticipar las brechas antes de que ocurran y su capacidad para responder rápida, decisiva y eficazmente a las brechas contrapuestas – maniobrando proactivamente los mecanismos de defensa en su lugar, antes y durante el ataque.

CTI se centra en la identificación y el análisis de las motivaciones, métodos, capacidades y herramientas de los adversarios que pueden tratar de apuntar hacia una organización mediante el análisis externo y comparado de los datos que una vez se segmentaron dentro de la empresa. Si bien algunas organizaciones pueden optar por definir el *CTI* como un único componente o un servicio impulsado por los insumos, es importante señalar que se requiere un ciclo de vida de inteligencia basado en procesos dentro de un marco operacional para proporcionar resultados accionables.

En consecuencia, se requiere un programa *CTI* integral y consistente en procesos para recolectar, producir y difundir inteligencia táctica y estratégica, continuamente aumentada con actualizaciones oportunas de la conciencia situacional (también conocida como inteligencia actual). Esto ayuda a explicar quién es el adversario relevante, cómo y porqué pueden estar atacando a la organización, qué acciones podrían tomar después del contacto inicial, dónde pueden residir dentro de la organización y cómo detectar o responder a un ataque.

El enfoque de EY para la inteligencia de amenazas cibernéticas



OSINT: Open Source Intelligence

***SMRs: Supplies Relationship Management*

¿Qué puede hacer la *CTI* por usted?

Es posible que las organizaciones ya estén invirtiendo en varias fuentes e informes de inteligencia, pero muchos todavía se preguntan: ¿qué puede hacer la inteligencia de amenazas cibernéticas por mí? La amplitud y diversidad de la respuesta de EY es a menudo sorprendente:

- **Inteligencia de amenazas cibernéticas es más que datos y tecnología, es la experiencia del analista, metodologías refinadas y procesos de integración:**

  La amplitud y diversidad del valor *CTI* no cae en cuenta cuando la inversión se realiza exclusivamente en datos y tecnología tales como amenazas de inteligencia de amenazas o plataformas de inteligencia. *CTI* debe integrarse en los procesos de seguridad y de negocios, adaptados a los desafíos únicos de la organización, y con el apoyo de analistas capacitados que utilizan una metodología rigurosa.

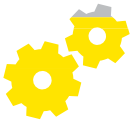
- **La inteligencia de amenazas cibernéticas representa un panorama más amplio para los encargados de tomar decisiones y coloca a los operadores de seguridad por delante del atacante cibernético:**

  A medida que el ecosistema tecnológico continúa ofreciendo un flujo de innovaciones disruptivas que tienen implicaciones positivas tanto para las organizaciones como para los individuos, el delincuente cibernético está descubriendo nuevas técnicas para atacar implacablemente cualquier cosa: desde dispositivos médicos hasta vehículos de motor que pueden conectarse a Internet.

  Frente a los crecientes ataques globales, las organizaciones pueden sentirse abrumadas por la cantidad de ruido relacionado con los ataques cibernéticos y los posibles impactos que esos ataques pueden tener para su negocio.

  Incluso cuando una organización posee datos de seguridad que podrían ser usados para informar a los tomadores de decisiones; la información a menudo se extiende a través del negocio de tal manera que, el establecimiento de una única visión centrada en el negocio del paisaje de amenazas de la organización, parece fuera de alcance.

87%



Perú

no tienen un programa de gestión de accesos e identidades.

Con la seguridad cibernética en la parte superior de la agenda en muchas salas de directorio, EY cree que las organizaciones requieren acceso a información estratégica a medida que informará a los líderes de las amenazas más destacadas que enfrenta su organización. *CTI* ofrece estas ideas integrando datos de seguridad previamente agrupados para proporcionar una perspectiva holística del paisaje de amenazas de la organización. Este enfoque integrado fortalece la postura de seguridad de la organización al empoderar a los *stakeholders* con una perspectiva informada sobre cómo las amenazas cibernéticas son relevantes para sus áreas de responsabilidad. Además, *CTI* puede potenciar un enfoque proactivo mediante la introducción de un marco operacional robusto para contrarrestar los adversarios, que incluye la estructura de gobierno adecuado y la madurez de las operaciones de seguridad.

- **La inteligencia de amenazas cibernéticas es el facilitador de enfoques de seguridad más proactivos:**

  Simplemente reaccionar a las acciones de un adversario cibernético contra su organización es sin duda una postura de seguridad no ideal. EY cree que adoptar un enfoque de defensa activa mejoraría la seguridad cibernética actual de una organización y concentraría las operaciones en evitar que los adversarios más probables de la empresa alcancen sus objetivos específicos (robo, fraude, manipulación del mercado, etc.). Este enfoque se realiza a partir de la visión generada por un programa integrado de transformación de seguridad cibernética combinado con el *CTI* analítico.

Defensa Activa

La parte "activa" de la Defensa Activa es realizada por la ejecución deliberada de conjuntos planificados de operaciones defensivas que se conocen como misiones. El uso del término misión hace que el proceso operacional se aplique con una cantidad significativa de análisis riguroso y disciplina para lograr una máxima eficacia en el cumplimiento de los objetivos de seguridad de la organización. Las misiones son planificadas en respuesta a amenazas específicas identificadas por la inteligencia en el contexto único de la organización defendida.

Los beneficios de la Defensa Activa son claros:

- Para el equipo de operaciones de seguridad, la Defensa Activa proporciona un conjunto definido de actividades de mejora racionalizadas por *CTI* y conectadas a objetivos alcanzables. El equipo construye contramedidas, caza intrusos ocultos y fortifica las defensas basado en informes reales sobre el comportamiento de atacantes reales.
- Para los responsables de la toma de decisiones, la Defensa Activa conecta la implementación de recursos directamente para medir la eficacia de las medidas del programa de seguridad cibernética. En lugar de centrarse en medidas de rendimiento como el número de parches aplicados y el número de los boletos cerrados, la efectividad es demostrada mediante una disminución del éxito de ataques dirigidos y una disminución en el tiempo necesario para descubrir y erradicar los ataques que tuvieron éxito.

Para obtener más información, consulte www.ey.com/activedefense

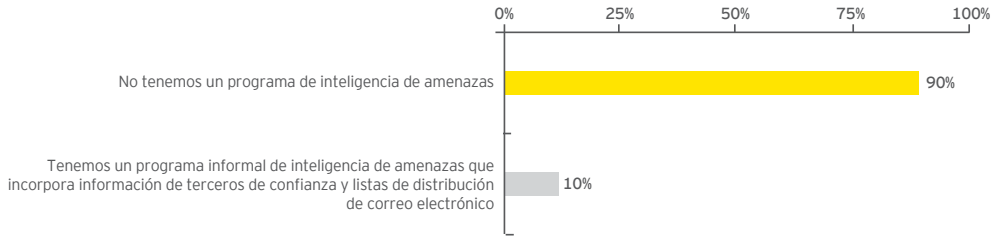
¿Cómo la industria está aprovechando la *CTI*?

Un marco operacional sólido garantiza que las operaciones de seguridad estén lo suficientemente maduras como para ingerir inteligencia relevante y realizar acciones oportunas. Un marco así necesitaría incluir más que la madurez tecnológica, sino también los procesos y la gobernabilidad que se abordan cuando una organización invierte en desarrollar una capacidad de inteligencia indígena, en lugar de solamente comprar mecanismos de inteligencia externos. Sin embargo, en muchas organizaciones estas consideraciones básicas del marco son a menudo pasadas por alto, o insuficientemente desarrolladas, para mantenerse al día con un panorama de amenazas dinámico y de cambio constante.

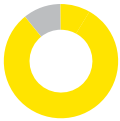
Una de las principales limitaciones que enfrentan las organizaciones al considerar una capacidad de *CTI* madura es el costo. Desarrollar una capacidad de inteligencia sólida puede ser costoso, lo que significa que encontrar el equilibrio adecuado de los servicios comprados y el crecimiento incremental es fundamental. Adicionalmente, los servicios adquiridos, como las suscripciones y las plataformas de inteligencia, vienen con su propio conjunto de desafíos: por ejemplo, estos tipos de servicios a menudo son adaptados a una audiencia técnica y carecen de enfoque en la industria. Esto representa un desafío para los ejecutivos que requieren un análisis centrado en el riesgo empresarial sobre las amenazas específicas de la industria que pueden aprovecharse para la planificación estratégica.

Mediante una visión basada en evidencias de la seguridad cibernética y el panorama de amenazas, la *CTI* puede ser entregada y aprovechada de muchas maneras para informar a los tomadores de decisiones en todos los niveles, desde analistas de seguridad hasta los más altos ejecutivos.

Estas fueron las respuestas de las organizaciones peruanas cuando preguntamos: ¿qué afirmación describe mejor la madurez de su programa de inteligencia de amenazas?



87%



Perú

no tienen un programa establecido de protección de datos.

Suscripciones

No todas las suscripciones de inteligencia de amenazas proporcionan lo mismo. Muchos proporcionan indicadores y reportes de bajo volumen y alta confianza; otros proporcionan volumen considerable con confianza variable; y algunos proveedores pueden enfocarse en un tipo de amenaza (por ejemplo, amenazas persistentes avanzadas, crimen cibernético o *hacktivismo*). Esta inteligencia puede provenir del análisis de la web oscura o de la web profunda, mecanismos propietarios de colección y/o análisis de información de código abierto.

El proceso de identificar y revisar información que es valiosa para una organización específica es desafiante debido al gran volumen de este tipo de fuentes abiertas, pagadas e internas. Incluso cuando se seleccionan fuentes y comienza la recopilación de datos, muchas organizaciones no son capaces de ingerir todo el alcance de lo que se proporciona (por ejemplo, Indicadores de Compromiso (*IOCs*)) o determinar la acción de informes pesados de información. Es importante destacar que el contexto de los informes de inteligencia suele estar ausente, dejando a la organización tratando de entender la relevancia y el trasfondo de por qué la información es importante.

Las suscripciones no deben limitarse únicamente a la integración automática de los reportes de inteligencia y la entrega electrónica de informes, sino que deben ser adaptadas a la industria y las necesidades de la organización para habilitar acciones. Esto puede lograrse gracias al trabajo del proveedor junto con la organización para, determinar la selección correcta de las ofertas de suscripción, que puede ser una combinación de:

- Reportes adaptados de indicadores técnicos para la integración automática
- Transmisiones web informativas y eventos de capacitación dirigidos a la operacionalización de la inteligencia de amenazas
- Reuniones informativas dadas por analistas para informar tanto a los operadores de seguridad como a los ejecutivos
- Reportes específicos de la industria y del negocio sobre eventos actuales, amenazas cibernéticas emergentes y tendencias en horarios personalizados para satisfacer las necesidades operacionales (diarias, semanales, etc.)
- Actualizaciones oportunas basadas en eventos con análisis de eventos cibernéticos importantes y relevantes

Tener un apoyo directo de los analistas para entregar productos, ofrecer sesiones informativas, responder a preguntas relacionadas con la inteligencia y adaptar el análisis y las recomendaciones al panorama de amenazas de una organización es fundamental para maximizar el uso de los servicios de suscripción.

Plataformas de inteligencia

Algunas soluciones de inteligencia de amenazas proporcionan una combinación de informes en una plataforma tecnológica que permite la visualización de datos, y con un gran número de proveedores de inteligencia de amenazas cibernéticas de los cuales elegir, las organizaciones pueden ser tentadas a seleccionar proveedores que ofrecen este tipo de solución pre-configurada e independiente porque estos tipos de vendedores están a menudo inmediatamente disponibles e inicialmente puede parecer más rentable. Sin embargo, al adquirir este servicio, las organizaciones a menudo se dan cuenta que han dejado que la información sea útil y relevante para ellos mismos, tienen poca propiedad de la información y corren el riesgo potencial de aumentar los honorarios de los contratos sin darse cuenta realmente del valor de su compra.

Las plataformas de inteligencia pueden ser un componente crucial para la seguridad cibernética cuando se combinan con procesos clave dentro de un programa maduro de inteligencia para visualizar datos recopilados y soportar tendencias a largo plazo. El análisis de tendencias puede proporcionar información valiosa y específica para la organización y la industria, mostrando cambios en el tiempo de las tácticas, técnicas y procedimientos (TTP) adversos y patrones de inteligencia de valor determinados cuando los *stakeholders* clave se toman el tiempo para documentar sus requerimientos de inteligencia. Este análisis es más efectivo cuando se capta de una manera que los líderes encuentran significativa la toma de decisiones de riesgos empresariales y la priorización de las contramedidas y actividades de remediación.

97%
Perú

afirman que las preocupaciones en cuanto a la seguridad de la información han ido aumentando y piensan emprender acciones en las estrategias y planes actuales.

Desarrollo del mercado de la *CTI*

El desarrollo de programas de *CTI* maduros dentro de un marco de seguridad cibernética, es la evolución natural de los servicios de inteligencia de amenazas más allá de las suscripciones, informes y plataformas técnicas compradas. Es una inversión a largo plazo que requiere dedicación y *stakeholders* claves que puedan darse cuenta de los beneficios duraderos que este tipo de servicio proporciona. Estas visiones a largo plazo entre los *stakeholders*, están emergiendo a pesar de conducir negocios en un mundo que promueve un valor inmediato menor a la seguridad cibernética sobre el crecimiento de una postura más madura y segura con el tiempo. Los servicios de inteligencia de este tipo incluyen un enfoque personalizado de gobernabilidad, personas, procesos, tecnología e información.

Una sólida integración de la *CTI* se basa en evaluaciones personalizadas que responden a preguntas específicas de los *stakeholders*, consideran el panorama de amenazas único de la organización y proporcionan un valor operacional inmediato con acciones exhaustivas recomendadas. Para apoyar esto, las organizaciones deberían considerar desarrollar un programa de *CTI* y también realizar una evaluación periódica de cómo el panorama de amenazas podría afectarlos.

▸ **Programas de *CTI***

Un programa de *CTI* ayudará a habilitar la capacidad dentro de la estructura de operaciones de seguridad de una organización para recopilar, analizar, producir e integrar su inteligencia propia y externa. El diseño, la construcción y el desarrollo de operaciones de un programa de *CTI*, apoyan el crecimiento simultáneo dentro de las operaciones de seguridad correspondientes, permitiendo a la organización ingerir inteligencia de amenazas cada vez más sólida, manteniendo al mismo tiempo al negocio de ser abrumado por la información: esto también les permite tomar acciones para las que están listos e identificar qué debe ser adicionalmente maduro para tomar medidas adicionales.

▸ Evaluaciones de *CTI*

En la actualidad, en el mercado hay brechas entre una organización que digiere la inteligencia de amenazas y una organización que luego integra la inteligencia en las operaciones. Un tema común es la frustración de dónde empezar.

La *CTI* se puede implementar de forma incremental, permitiendo pequeñas inversiones para mejorar y madurar otras áreas de la gestión de amenazas cibernéticas de una manera que maximice el retorno de la inversión.

Las evaluaciones personalizadas recogen los hechos pertinentes y organizan los pros y los contras de diversos atributos del programa para promover un enfoque orientado al proceso, proporcionando ideas inmediatas y una mirada evaluada en donde las organizaciones pueden comenzar a integrar *CTI*. Estas evaluaciones pueden responder a preguntas de negocios específicas, proporcionando un camino despejado hacia adelante a través de recomendaciones.

El caso para poner en funcionamiento la *CTI*

Un desafío común que existe en la industria es cómo hacer uso de la *CTI* de la mejor manera:

- ¿Cómo puede una organización hacer a la *CTI* relevante y accionable?
- ¿Cómo puede una organización integrar inteligencia relevante y procesable en las operaciones de seguridad?

Comprar suscripciones, informes y/o reportes de inteligencia de amenazas no responde a estas preguntas, tampoco lo hace la instalación de una plataforma de inteligencia de amenaza de vanguardia. Sólo a través del desentierro de los requisitos de la *CTI* única de una organización y el diseño de procesos de integración personalizados, puede realmente poner en funcionamiento la *CTI*.

Sin embargo, EY ha señalado varias cuestiones que limitan el funcionamiento de la *CTI*. Un problema es la falta de consolidación de las fuentes de inteligencia (es decir, múltiples suscripciones propiedad de la organización utilizadas por diferentes divisiones y no compartidas). Otro problema es la incapacidad de mantener las plataformas o integrar los resultados de inteligencia en los aparatos archivados; otras organizaciones pueden tener una incapacidad para integrar adecuadamente las fuentes de inteligencia adquiridas en las tecnologías de seguridad, lo que limita la capacidad de usar la inteligencia comprada de manera significativa.

Poner en funcionamiento la *CTI* es necesario para derivar algo más que una falsa sensación de seguridad por haber leído un informe o haber comprado un reporte de inteligencia.

Requerimientos de inteligencia

Los requisitos de inteligencia son la forma en que una organización dirige y alcanza sus esfuerzos de la *CTI* con el fin de asegurar que adquieran la visión correcta y la capacidad de poner en funcionamiento la inteligencia. Los requisitos son preguntas específicas y singulares que una organización no tiene actualmente: respuestas incompletas o que no agregarán valor al negocio. Los requisitos deben ser desarrollados en base a múltiples operaciones, preocupaciones y brechas en el conocimiento de los *stakeholders*. De esta manera, los requerimientos de inteligencia tomarán la forma y la sensación de la organización y serán igualmente únicos y diversos. Por ejemplo, una organización manufacturera con presencia mundial tendrá requisitos de inteligencia relacionados con la cadena de suministro global, mientras que una organización financiera regional puede que no.

26%
Perú

piensa que es altamente probable que la pérdida de la información confidencial corporativa en dispositivos móviles, aumenta el presupuesto de seguridad de la información.

90%
Perú

piensa que es altamente probable que la pérdida de la información personal a través de dispositivos móviles, aumente el presupuesto de seguridad de la información.

Al identificar preguntas específicas que necesitan ser resueltas en una organización, puede orientar la recolección y producción de inteligencia para apoyar las operaciones y toma de decisiones

La recolección de inteligencia debe tener lugar tanto interna como externamente a la organización. La información interna recopilada podría incluir información de eventos de red, información de escaneo de vulnerabilidades e informes de respuesta a incidentes. La información obtenida externamente podría incluir actividades en la web profunda y oscura, discusiones en medios de comunicación y en foros, noticias geopolíticas y reportes de terceros sobre los adversarios y sus actividades.

Muchas empresas optan por comprar sus inteligencias derivadas externamente a través de suscripciones y reportes. Hay tantas opciones y combinaciones de información externa e interna para recopilar qué decidir, qué recoger o comprar, que puede parecer desalentador. Muchas organizaciones terminan con fatiga de información y cantidades significativas de información de las que no están haciendo uso, lo que resulta en una ausencia de *CTI* en funcionamiento. Al pre-definir los requisitos de inteligencia, una organización puede concentrar sus esfuerzos y determinar la sección transversal más relevante de las fuentes recopiladas para la organización.

No basta con recolectar los datos, sino que deben usarse para plantear un escenario más amplio de lo que está ocurriendo en el panorama de amenazas de la organización. Para ello, los datos deben ser monitoreados, analizados, tendidos, cuantificados en métricas y luego entregados a la audiencia apropiada para que puedan tomar acción - informes diarios, semanales, mensuales, trimestrales, anuales e incluso bajo demanda - pueden servir para completar esta imagen.

La producción de inteligencia debe responder a las preguntas de diferentes grupos de *stakeholders* con el nivel correcto de detalle operacional, de manera oportuna y en un formato fácil de entender. De esta manera, los informes de compras, que se venden a varias organizaciones, a menudo no tienen en cuenta las necesidades operativas específicas de éstas y es por esta razón que cada vez más organizaciones preguntan cómo hacer uso de los informes de inteligencia sobre amenazas. Las respuestas se encuentran en los requisitos definidos unívocamente, la recolección focalizada y la producción impulsada por operaciones.

Utilizando la inteligencia para apoyar a toda la organización

La inteligencia de amenazas cibernéticas apoya conjuntamente a los tomadores de decisiones y a las operaciones de seguridad

La *CTI* acumulada y producida debe integrarse a través de procesos diseñados para apoyar tanto a los tomadores de decisiones como a las operaciones de seguridad. Los procesos de entrada y productos de salida de un programa *CTI* deben ser diseñados con el objetivo de mejorar la concientización sobre amenazas cibernéticas en toda la organización y en una variedad de niveles. EY cree que esto puede lograrse cuando la *CTI* se vea desde la perspectiva de los componentes de inteligencia táctica, estratégica y actual y entregada a los *stakeholders* relevantes.

Componentes del programa *CTI*

Inteligencia Táctica

- Actúa como un multiplicador de fuerza para las operaciones de seguridad interna que mejoran la postura de amenaza organizacional
- Otorga inteligencia técnica que puede ser rápidamente integrada en un sensor propio de la organización y capacidades para la primera línea de defensa
- Aprovecha el análisis del ciclo de vida del adversario para reunir varias funciones de sus operaciones

Inteligencia Estratégica

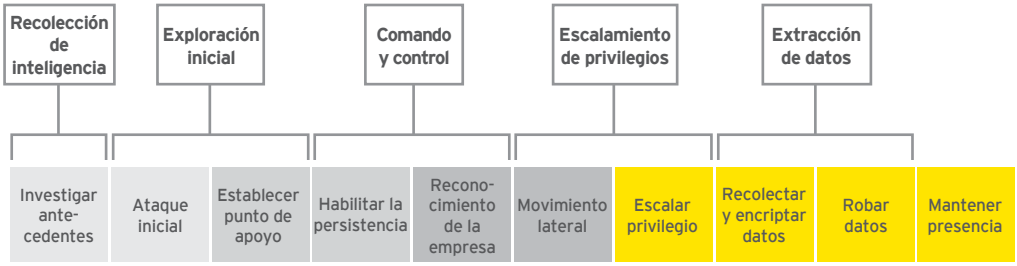
- Traduce las amenazas cibernéticas en riesgos de negocio
- Empodera a los tomadores de decisiones para priorizar acciones estratégicas a corto plazo

Inteligencia Actual

- Muestra rápidamente avisos tempranos de las últimas amenazas a los *stakeholders* en toda la organización
- Conduce funciones de inteligencia ágiles, flexibles, estratégicas y tácticas
- Analiza en el mismo día las vulnerabilidades emergentes con acciones de remediación sugeridas

- **Los procesos de análisis de inteligencia de nivel estratégico** que apoyan directamente las operaciones del negocio, incluyen el análisis de priorización, evaluaciones de riesgo y análisis predictivo. Todos estos procesos analíticos requieren conjuntos de datos sólidos y suponen una tendencia y un análisis minucioso que proporciona información valiosa que puede apoyar a los responsables a la toma de decisiones.

- **Los procesos de análisis de inteligencia en un nivel táctico** apoyan directamente a los *SOCs* en torno al análisis del ciclo de vida del adversario.



Al analizar la actividad del adversario en torno al ciclo de vida de las acciones tomadas por el criminal cibernético, los analistas de la *CTI* táctica pueden:

1	Integrar las tácticas, técnicas y procesos de adversarios conocidos a varias operaciones de seguridad
	a. Enfocar esfuerzos más precisos para identificar las actividades de los adversarios a tiempo en su ciclo de vida **b.** Enfocar los esfuerzos para localizar a los adversarios e identificar daños después de la infracción

2	Desarrollar modelos de amenazas que ilustren las posibles actividades del adversario
	a. Analizar a los adversarios que pueden afectar a la organización, los activos a los que pueden apuntar y los caminos en la red que el adversario puede tomar **b.** Fijar modelos de amenazas para atacar y proveer profesionales de penetración que activamente simulen ataques similares

3	Crear una primera línea de defensa para la colección de redes derivadas internamente
	a. Recolectar datos esenciales de eventos en la red que apoyen tendencias y análisis estratégicos **b.** Proporcionar información sobre la actividad de la red más allá de la longitud de la captura de registro

- **Los procesos de inteligencia actuales** apoyan tanto a las operaciones de negocio, como a las operaciones de seguridad; centrándose en obtener los datos más oportunos y un análisis rápido para varios analistas y *stakeholders*. Los actuales analistas de inteligencia son la primera línea de defensa para identificar inteligencia externa relevante y dirigirla a las partes que necesitan operacionalizar. De esta manera, la inteligencia actual es fundamental para asegurar la operacionalización oportuna de *CTI*.

Todos los niveles de inteligencia se operacionalizan en remediaciones y acciones de contramedida. De hecho, las acciones de contramedida impulsadas por la inteligencia, son un principio rector del punto de vista de EY sobre **Defensa Activa** - una campaña deliberadamente planificada y continuamente ejecutada, para identificar y erradicar a los atacantes ocultos, y derrotar los posibles escenarios de amenazas dirigidos a sus activos más críticos.

Las acciones de remediación y contramedida impulsadas por la inteligencia incluyen procesos que permiten la operacionalización de *CTI*:

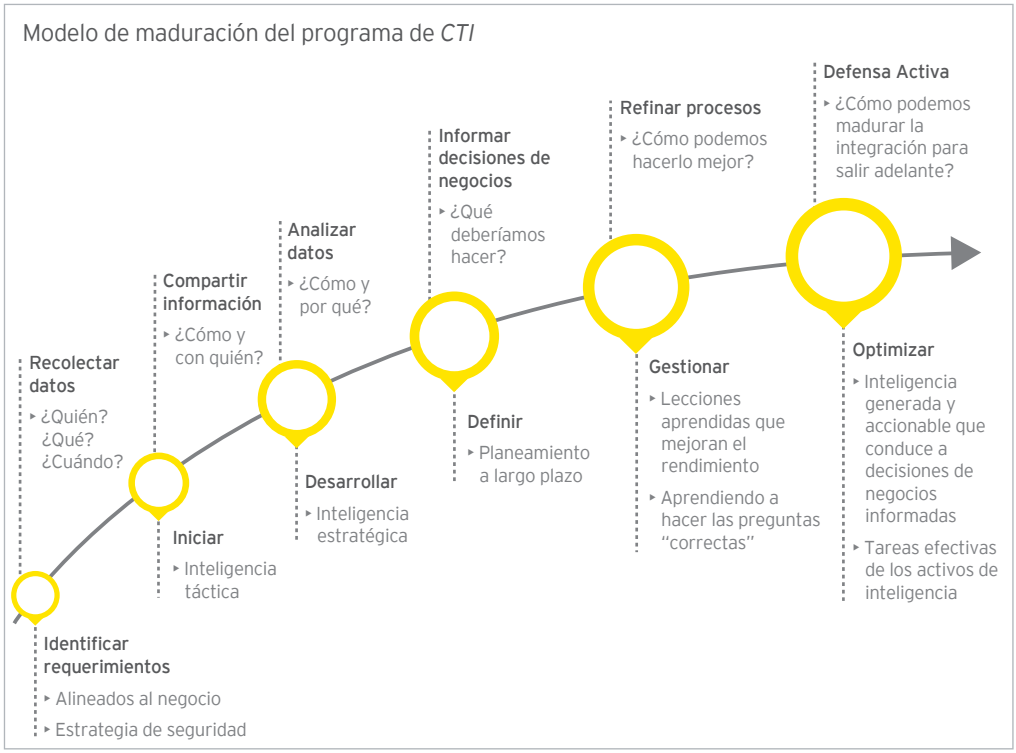
- Apoyo de la inteligencia de amenazas para los planes de respuesta a incidentes
- Alerta y recomendación de acciones para la inteligencia actual investigada
- Orientación de las operaciones de seguridad a lo largo de los caminos de los modelos de amenaza desarrollados.

El caso para *CTI* – Escenario de ejemplo

Con el rápido cambio del panorama de amenazas y el impacto de los ataques aparentemente cada vez más altos, adelantarse a posibles ataques y vulnerabilidades ha sido un gran logro para algunas organizaciones que han mejorado sus capacidades de *CTI*. Para muchas organizaciones sin una idea de lo que está cambiando, obtener preguntas de pánico de los ejecutivos puede hacer de una situación ya complicada, mucho más estresante.

Durante varias de las recientes brechas se usó un vector de ataque o de vulnerabilidad. Los equipos de seguridad de las organizaciones no sólo pudieron resolver dichos problemas sino que, en algunos casos, se adelantaron a las discusiones con una llamada para establecer que tenían conocimiento de lo que estaba ocurriendo, siendo capaces de determinar si estaban asegurados contra la amenaza específica, o en su defecto, lo que estaban haciendo los equipos para remediar la situación rápidamente.

Todos estos procesos serán únicos para las operaciones y retos de su organización



Conclusión

El futuro de la inteligencia de amenazas cibernéticas

A pesar de que la *CTI* no se ha proliferado plenamente en el mercado, las organizaciones necesitarán seguir adaptándose al cambio en el panorama de las amenazas cibernéticas para comprender mejor cómo la inteligencia de amenazas puede reducir su riesgo de negocio en general. Las discusiones de *CTI* que rodean el riesgo del negocio, más que sólo el riesgo de seguridad, se volverán cada vez más comunes. La comprensión de los riesgos de amenaza cibernética para las finanzas, la reputación, la información y las operaciones del negocio continuará ampliando la discusión más allá de una audiencia de seguridad o tecnología.

Las organizaciones presionadas y de corto alcance seguirán comprando informes y tecnologías de inteligencia de amenazas, sin alinear tales inversiones con una visión a largo plazo de la gobernabilidad, los procesos integrados y los requisitos empresariales únicos. Sin embargo, cada vez más empresas comenzarán a concentrarse en la construcción de una sólida capacidad de inteligencia de amenazas y/o hacer uso de inteligencia adaptada para responder a sus preguntas específicas de negocios. Esto conducirá a mayores inversiones en el diseño del proceso que rodea a la *CTI* y la adaptación de inteligencia de amenazas de la industria u organización.

Las principales organizaciones se centrarán más en la personalización de la *CTI* disponible por su cuenta, y estarán más dispuestas a compartir inteligencia de amenazas con otros en su entorno para hacer que esta sea factible. Esto conducirá a un mayor disgusto por la protección propietaria del contexto de inteligencia valioso de los vendedores de inteligencia. A su vez, los proveedores de la *CTI* deberán centrarse más en proporcionar detalles sobre cómo opera el adversario (indicadores dinámicos) que en compartir indicadores singulares de compromiso (indicadores estáticos) que carecen de contexto.

Los sectores financiero y gubernamental seguirán liderando el camino de la integración de la *CTI* basada en el proceso y el intercambio de información. Las industrias con mayor riesgo y desafíos únicos, como el petróleo y gas, el comercio minorista, el cuidado de la salud, la alimentación y la agricultura, aumentarán las inversiones en el área de la *CTI* y, como estas industrias continúan evolucionando sus capacidades de inteligencia de amenaza, sin duda contribuirán al desarrollo de las mejores prácticas en la seguridad cibernética.

La *CTI* ayudará a las organizaciones a aprovechar los conceptos de seguridad de la próxima generación, tales como: modelado de amenazas, Defensa Activa y operaciones avanzadas de contramedida. El objetivo será desarrollar procesos repetibles que sean efectivos para todas las organizaciones en la transición de una postura de seguridad reactiva a un enfoque proactivo. Las organizaciones apreciarán mejor la necesidad de entender su propio entorno a un nivel mucho más profundo para lograrlo.

Se incrementarán las inversiones en el mapeo detallado de entornos en red, el almacenamiento a largo plazo y visualización de información de operaciones de seguridad, la identificación y valoración de activos de alto valor, la gobernanza y el diseño de procesos que rodean las capacidades de seguridad actualmente unidas, los juegos de azar de escenarios cibernéticos contra tales activos, y la comprobación de las contramedidas.

Las amenazas cambian con el tiempo, al igual que los riesgos. EY cree que los procesos de la *CTI* pueden ayudar a las organizaciones a adelantarse a esas amenazas, mitigar los riesgos y, por último, asegurar el éxito de la organización.

¿Cómo puede ayudar EY?

EY proporciona servicios de asesoramiento de *CTI* en torno a evaluaciones, compilaciones de programas, soporte de programas y servicios de suscripción a clientes de todo el mundo. También puede permitir una integración perfecta para las organizaciones que desean integrar inteligencia de amenazas cibernéticas de terceros en sus operaciones de seguridad. Adicionalmente, EY puede ayudar a cerrar la brecha entre los aspectos tácticos y técnicos de la *CTI* y ayudar a habilitar más discusiones estratégicas que afectan la toma de decisiones empresariales.

A lo largo del desarrollo y maduración de un programa de *CTI*, EY:

- Apoya a los clientes en la maduración de sus procesos para ser capaces de ingerir inteligencia de amenazas cada vez más robusta
- Ayuda a crear la capacidad interna de traducir inteligencia técnica en puntos de vista estratégicos para los tomadores de decisiones empresariales
- Ayuda a evitar que los clientes se ahoguen en información y produce inteligencia relevante
- Proporciona una mirada personalizada al escenario de amenazas de nuestros clientes e identifica lo que debe ser madurado para tomar nuevas medidas
- Identifica oportunidades internas y externas de intercambio de información claves
- Asiste en la selección de tecnología y la arquitectura de soluciones

III.

Respuesta ante incidentes

Introducción

Una eventualidad inevitable

La realidad de hoy en día

No es un crimen ser atacado; no se puede dejar de ser un objetivo. No es un crimen ni siquiera ser objeto de una irrupción. Las amenazas vienen de muchas direcciones y son altamente sofisticadas. El verdadero problema es no darse cuenta de haber sido atacado y no reaccionar de manera planificada y coordinada.

Como muchas organizaciones han aprendido - a menudo de la peor manera - los ataques cibernéticos son inevitables y las irrupciones sucederán. Los atacantes son cada vez más implacables: cuando una táctica falla, los adversarios intentarán otros métodos hasta romper las defensas de una organización. Al mismo tiempo, la tecnología está aumentando la vulnerabilidad de las empresas, y los ataques tienen una mayor presencia en línea, un uso más amplio de los medios sociales, una adopción masiva de dispositivos móviles, un mayor uso de servicios en la nube y de terceros, y una recopilación y análisis de grandes datos.

Los ataques cibernéticos son complejos y motivados por factores complejos que van desde una ideología y ganancia financiera hasta el espionaje corporativo e incluso agendas impulsadas por los estados. Las amenazas están en constante evolución, dirigidas a todas las industrias, a la vez que se vuelven más frecuentes y de alto nivel. Los delincuentes cibernéticos de hoy en día son pacientes, persistentes y sofisticados y atacan no sólo a la tecnología sino también a las debilidades de las personas y de los procesos.

Las organizaciones que se preparan para los inevitables ataques cibernéticos pueden estar en mejor condición para reaccionar eficazmente y gestionar el daño a su marca después de la irrupción. Sin embargo, existen una serie de desafíos:

- Los ataques a gran escala no suceden todos los días, por lo que es difícil mantener el nivel necesario de vigilancia y preparación para poder responder en cualquier momento.
- Responder rápidamente, de una manera tranquila y estructurada, es muy difícil sin planificación previa.
- Detectar un ataque continuo antes de que se convierta en una irrupción puede ser casi imposible sin capacidad de monitoreo de seguridad.

42%

Global

35%

Perú

no cuenta con una estrategia o plan de comunicación en caso de una ataque significativo.

- Los pasos tomados en los primeros momentos de una respuesta a un ataque son críticos para el éxito de la respuesta. Sin embargo, muchas decisiones clave deben tomarse rápidamente con información incompleta.
- La gestión de múltiples interesados en un momento de crisis es vital, y a la vez desafiante. La mayoría de las partes interesadas de las organizaciones incluyen a la compañía, su junta directiva y accionistas, sus empleados y clientes, reguladores, medios de comunicación y aseguradoras.
- Llegar a un equilibrio entre las capacidades de respuesta internas de la empresa y las que puedan tercerizar puede ser difícil, pero debe determinarse previamente a una irrupción.

Las organizaciones que tienen un plan de respuesta a ataques, que ha sido probado con un equipo experimentado, pueden reducir significativamente el impacto de una irrupción.

Una infinita gama de ataques

35%
Perú

no tienen una estrategia o plan contra ataques cibernéticos significativos.

El intruso silencioso de hoy

Muchos ataques, como la negación de servicio (*denial of service*), son evidentes y perturbadores, haciéndolos fáciles de detectar. Los ataques más dañinos consisten en múltiples fases y emplean métodos sofisticados y discretos que permanecen sin ser detectados por largos períodos de tiempo. Estos tipos de ataques se conocen comúnmente como amenazas persistentes avanzadas (*advanced persistent threats - APT* por sus siglas en inglés).

1. El atacante recopila información sobre el objetivo para identificar *targets* y vulnerabilidades aprovechables.

2. El atacante comienza a prestar especial atención a los sistemas, vigilando cualquier signo de vulnerabilidad. Los ataques pueden incluir *phishing*, explotación de vulnerabilidades, ingeniería social, etc.

3. Una vez establecido, el atacante comienza a propagarse a través de los recursos de TI de la organización. Esto proporciona una *beachhead* y abre una gran variedad de oportunidades para que un atacante pueda pasar de un sistema a otro, ocultando su presencia.

4. El atacante obtiene acceso a los recursos de TI de la empresa: ahora tratará de obtener mayores privilegios instalando herramientas maliciosas adicionales, comprometiendo nuevos sistemas, entre otros.

5. El atacante identifica información útil y valiosa, tratando de extraerla de los sistemas de la empresa, y puede usar un enfoque de perfil bajo descargando pequeñas cantidades de datos (o limitando la velocidad de descarga) para evitar su detección por los sistemas de monitoreo de red.

La única manera de responder eficaz y eficientemente a este tipo de ataques es preparándose, tanto en términos de un plan de respuesta como de un equipo que haya sido entrenado y que se someta a pruebas periódicas. Una detección y una respuesta oportunas también pueden ayudar a desbaratar a los atacantes activos antes de que puedan provocar un daño real.

Una respuesta efectiva

A continuación se describe el proceso de respuesta típico, basado en las prácticas líderes.

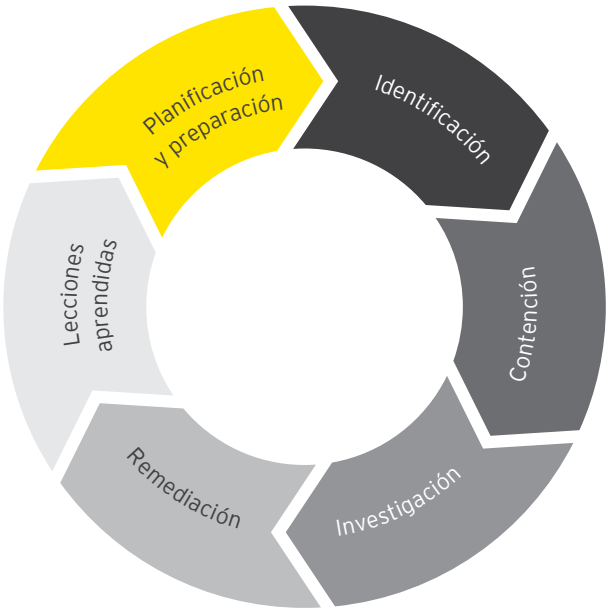
Sin embargo, para ser eficaz, una organización debe tener un plan de respuesta que se adapte a ella. Las áreas específicas de una organización incluirán: sus activos críticos, las amenazas más probables de ser reconocidas, sus procesos de identificación y detección, los criterios de toma de decisiones y las líneas de reporte, además de los miembros del equipo y las tecnologías que los soportan.

81%
Global

hace su propia investigación de incidentes.

83%
Global

hace su propio análisis de inteligencia de amenazas.



Es de crucial importancia la identificación e interacción con terceros, tanto los que participan en negocios regulares con la empresa, como aquellos abogados especializados y organismos reguladores que pueden estar involucrados en casos de una irrupción. Las organizaciones con capacidades avanzadas de seguridad cibernética aprovecharán el modelo de amenazas cibernéticas para no sólo identificar las principales amenazas, sino también preparar respuestas y contramedidas. Un plan de respuesta centrado exclusivamente en TI y dirigido por el departamento de TI de la organización está destinado al fracaso. Una respuesta eficaz involucra a todos los aspectos de la empresa, desde el *CEO* hasta Recursos Humanos, asesoría general, medios, entre otros.

Ciclo de vida de respuesta a incidentes de alto nivel

Las fases de respuesta ante incidentes (*Incident Response - IR* por sus siglas en inglés) se llevan a cabo típicamente en orden. Sin embargo, es habitual que la *IR* general sea de naturaleza iterativa, con algunas fases que se repiten a medida que la *IR* avanza y se obtiene información adicional.

Planeamiento y preparación

- Identificar escenarios especialmente probables o especialmente dañinos para enfocar el esfuerzo inicial en áreas de mayor riesgo.
- La *IR* debería incluir planes de desarrollo, creación de equipos y capacitación, así como establecer tecnologías de apoyo.
- Regularmente probar el plan o equipo (simulación de ataques cibernéticos).

Identificación

- Detectar e identificar una intrusión.
- Triaje, categorización y clasificación de un incidente, y decisión sobre medidas de contención inmediatas.
- Establecer un gabinete, montar *IR*, realizar una evaluación detallada y formular un plan de acción específico.
- Confirmar roles y responsabilidades y establecer líneas de reporte y frecuencia de estos.

Contención

- Determinar los pasos a seguir para contener el daño o riesgo que representa un ataque.
- Documentar el plan de contención y, si es posible, probar los controles técnicos de contención.
- Implementar los controles de contención y monitorear la efectividad o impactos adversos.

Investigación

- Identificar fuentes de evidencia potencial y preservarlas, según sea necesario.
- Procesar y analizar la evidencia relevante al incidente y determinar la causa raíz del mismo.
- Informar y realizar actividades de seguimiento para apoyar litigios, seguros y respuestas regulatorias.

La fase de investigación suele ser un proceso iterativo que se ejecuta en paralelo con la mayoría de las otras fases; en particular, la alimentación en la contención, la erradicación y la recuperación.

Remediación

- Desarrollar e implementar un plan para remediar la causa del incidente y devolver la organización a un estado estable.
- Documentar los planes y los controles y, si es posible, probar los métodos de remediación técnica.
- Desplegar controles de remediación y reconstruir los sistemas.
- Monitorear los incidentes y los impactos adversos.

Lecciones aprendidas

- Finalización de recopilación de datos de *IR* así como llevar a cabo reuniones para compartir las lecciones aprendidas.
- Proporcionarle retroalimentación a los miembros del equipo y actualizar el plan de *IR* con mejoras.
- Implementar mejoras a largo plazo en materia de seguridad, para ayudar a reducir el impacto de incidentes similares en el futuro.

Cómo puede ayudar EY

Creemos que la respuesta a incidentes es un proceso continuo que beneficia a las organizaciones cuando ejecutan tanto enfoques proactivos como reactivos. En lugar de tomar medidas después de una intrusión, EY lo ayuda a fortalecer su programa de respuesta a incidentes de modo que una vez que un ataque se produce, se puede mitigar con eficacia para reducir el impacto.

Nuestro enfoque sigue un ciclo iterativo de evaluar, mejorar y operar.

Evaluar

Esta fase consiste en evaluar la capacidad de respuesta de una organización ante un incidente, lo cual puede implicar una serie de actividades, entre ellas:

- **Evaluación del estado actual**

  Para las organizaciones que tienen una capacidad de respuesta ante incidentes, podemos evaluar la madurez de sus capacidades y proporcionar recomendaciones para mejorarlas.

- **Simulación de incidentes cibernéticos**

  Realizar un ejercicio de simulación para evaluar la madurez y la efectividad de un plan de respuesta ante incidentes a través de un escenario de ataque cibernético dirigido a la organización.

- **Juegos de guerra en vivo**

  Aprovechamos nuestros "equipos rojos" de ataque y penetración de nuestro Centro de Seguridad Avanzada (*Advanced Security Center - ASC* por sus siglas en inglés) para ayudar a evaluar la real habilidad de la organización para detectar y responder a ataques premeditados.

- **Diagnóstico de compromiso cibernético**

  Esta actividad ayuda a una organización a detectar cualquier actividad sospechosa en su red, así como el impacto potencial en el negocio.

Mejorar

Trabajamos con nuestros clientes para identificar una capacidad efectiva y eficaz de respuesta a incidentes. Esto cubre personas, procesos y tecnología. Las actividades en esta fase incluyen:

- **Desarrollo y mejora del plan de respuesta a incidentes**

  Ayudamos a desarrollar un plan de respuesta adaptado a la organización. Esto inicia por definir sus activos críticos, comprender las amenazas más probables mediante el modelo de amenazas, personalizar el proceso de identificación y detección, preparar planes de contención, investigación y remediación para los ataques más probables; y definiendo claramente roles y responsabilidades del equipo. Los terceros críticos también son mapeados y comprometidos.

- **Establecer tecnologías de apoyo**

  Asistimos en la selección e implementación de tecnologías de detección, como las ubicadas en el centro de operaciones de seguridad (*SOC*) de una organización, además de las tecnologías utilizadas para preservar y recopilar datos probatorios.

- **Entrenamiento y pruebas**

  Proporcionamos capacitación a las áreas relevantes y luego facilitamos tanto los juegos de guerra en vivo así como las simulaciones de incidentes cibernéticos a nivel *C-suite*, que ponen a prueba el equipo y el plan de respuesta en un escenario real adaptado a la organización. Esto proporciona un entorno seguro para que los miembros del equipo adquieran experiencia vital y puedan resolver cualquier aspecto del plan que de otra manera sólo se identificará durante un incidente.

Operar

Independientemente de las capacidades de una organización, podemos ayudar cuando ocurre lo peor. En esta fase, adaptamos nuestro enfoque a la organización del cliente:

- **Participar con anticipación**

  Nuestra preferencia es establecer una relación con nuestros clientes antes de un incidente y ayudarles a prepararse, ya que esto contribuye a una respuesta más controlada. Podemos establecer acuerdos de nivel de servicio (*SLAs*) y términos y condiciones (*T&Cs*) de manera anticipada.

- **Dirigir o co-elaborar la respuesta**

  Podemos proporcionar asistencia de respuesta rápida para el ciclo de vida de respuesta ante incidentes. Muchos de nuestros clientes simplemente solicitarán nuestra asistencia en la fase de investigación, mientras que otros solicitan que designemos un administrador de incidentes para que ejecute todo el proceso. Nuestro enfoque estructurado y metodológico tiene en cuenta la naturaleza variada de las intrusiones cibernéticas, permitiéndonos asistirlos sin importar la situación.

¿Por qué EY?

Trabajamos con nuestros clientes en sus momentos más difíciles proporcionando asesoramiento y capacidades de respuesta práctica, para ayudar a reducir el impacto de un incidente y llevarlos a una conclusión de una manera segura y eficiente. Juntos, nuestros enfoques proactivos y reactivos, ayudan a madurar su capacidad global de respuesta ante incidentes. Las lecciones aprendidas de los incidentes y las iniciativas proactivas se evalúan constantemente para su eficacia, para mejorar su eficiencia y se ponen en funcionamiento para mitigar los ataques cibernéticos en el futuro.

Nuestro alcance global nos permite escalar a la perfección cuando un incidente aislado se convierte en una irrupción internacional. Nuestros equipos están formados por personal de respuesta ante incidentes, profesionales de la tecnología e investigadores; todos con experiencia en situaciones de respuesta rápida y conocedores de los ambientes de negocios complejos en los que las organizaciones ahora operan.

Para los clientes que no requieren tecnología interna, podemos ayudar a implementar servicios de respuesta ante incidentes y utilizar tecnología forense para contener, investigar y remediar incidentes.

Ubicaciones de equipos de respuesta a incidentes

Forensic data centers (Centros de data forense)

Advanced security centers (Centros de seguridad avanzada)

Forensic evidence labs (Laboratorios de evidencia forense)

IV.

Seguridad cibernética y el Internet de las Cosas

Introducción

El crecimiento y la difusión de la interconexión digital

El rápido cambio tecnológico ha dado lugar a que muchos aspectos de nuestras vidas estén interconectados y afectados por las comunicaciones digitales.

Con miles de millones de personas conectadas a Internet hoy en día, y el pronóstico del número de dispositivos conectados para el año 2020 superando los 50 mil millones, el Internet de las Cosas (*Internet of Things - IoT* por sus siglas en inglés) representa una transformación importante en un mundo digital que tiene el potencial de afectar a todos y a cada negocio.

El *IoT* puede definirse como objetos físicos que se conectan a Internet a través de sistemas y sensores integrados, interactuando con él para generar resultados significativos y conveniencia para la comunidad de usuarios finales. El *IoT* ayudará a habilitar un entorno con la flexibilidad de proporcionar servicios de todo tipo, desde la automatización del hogar hasta la venta y logística inteligente; y desde el monitoreo ambiental inteligente hasta los servicios inteligentes de la ciudad.

En muy poco tiempo, el *IoT* contará con herramientas de detección, análisis y visualización a las que pueda acceder cualquier persona, en cualquier momento y en cualquier parte del mundo; a nivel personal, comunitario o nacional. El potencial de poder facilitar cualquier aspecto de nuestras vidas es lo que está estimulando que esta idea se establezca y prospere.

Sin embargo, el cambio real no es que las máquinas estén hablando entre sí, sino que la gente está hablando cada vez más a través de máquinas - el *IoT* es en realidad el medio de interconexión para las personas - y debido a que la comunicación humana se realiza a través de dispositivos IT y es cada vez más indirecta, hay un problema de seguridad profundamente arraigado con la posibilidad de suplantación y robo de identidad, *hacking* y, en general, amenazas cibernéticas.

El *IoT* dependerá cada vez más de la computación en la nube y de los dispositivos inteligentes con sensores incorporados junto con miles (si no millones) de aplicaciones para apoyarlos. El problema es que los entornos verdaderamente integrados necesarios para soportar esta tecnología conectada, aún no existen y la computación en la nube necesita seriamente una mejora, especialmente en términos de seguridad.

La movilidad, los modelos de negocio digitales, las infraestructuras energéticas inteligentes, la adopción de tecnologías de punta, las tecnologías de vanguardia para el transporte, los bienes de consumo y los servicios, están transformando los problemas de seguridad cibernética. Del *backoffice* a la vanguardia de la calidad del servicio y el desarrollo de negocios, la seguridad está ahora integrada en las estrategias básicas de un negocio líder.

No hay un solo objeto que se pueda describir como el modelo de infraestructura del *IoT*, hay muchas redes e infraestructura dispares y desiguales. Debido al aumento de estas redes y a las demandas de los datos que necesitan ser utilizados, muchas áreas técnicas tendrán que ser rediseñadas. Además, el número de dispositivos conectados en circulación que se utilizan para la gran cantidad de interacciones, ha creado nuevos retos en la privacidad y la protección de datos, la seguridad, la gobernanza y la confianza.

Teniendo en cuenta todos estos factores, vemos oportunidades y desafíos que requieren una atención especial y, en particular, la necesidad de un enfoque estratégico integral de la seguridad cibernética. Este informe destaca porqué estar en una posición proactiva para anticipar y mitigar la amenaza cibernética, es uno de los objetivos empresariales más importantes de hoy.

¿Qué es el Internet de las Cosas (*IoT*)?

El Internet de las Cosas (*IoT*) es la red de objetos físicos que contiene tecnologías integradas para comunicarse e interactuar con sus estados internos o con el entorno externo.

El Internet de las Cosas, Gartner IT. (Dakota del Norte). Obtenido de: http://www.gartner.com/it-glossary/internet-of-things

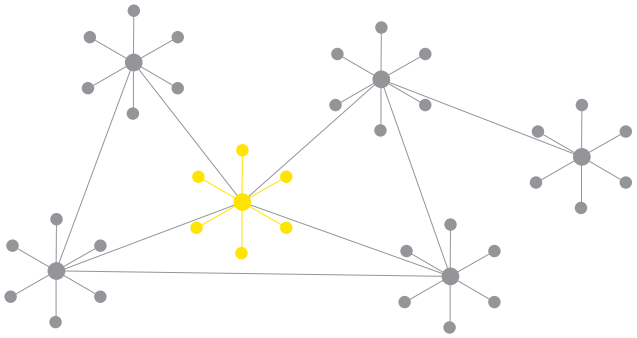
El *IoT* es un desarrollo futuro de Internet en el que los objetos y sistemas vienen incorporados con sensores y capacidad de procesamiento, con la intención de poder comunicarse entre sí. Aunque el concepto original del *IoT* pone excesivo énfasis en las comunicaciones de máquina a máquina, el verdadero resultado es la diversificación e incremento de las comunicaciones entre las personas de manera cada vez más indirecta. Las máquinas pueden eventualmente ser capaces de comunicarse, pero hasta el momento este fenómeno no es universal ni abarca todos los tipos de redes; incluso cuando las máquinas pueden conectarse entre sí, el hecho es que permanecerán como instrumentos de las comunicaciones humanas.

Las crecientes capacidades de conexión a red de las máquinas y dispositivos en el hogar, equipos de oficina, tecnologías móviles y portátiles, vehículos, fábricas enteras y cadenas de suministro, e incluso infraestructura urbana, abren un enorme campo de juego de oportunidades para la mejora del negocio y la satisfacción del cliente.

La mayoría de los dispositivos del *IoT* utilizarán tecnologías basadas en sensores en las que éstos identificarán o medirán cualquier cambio de posición, ubicación, entre otros; estos sensores transmitirán datos a un dispositivo o servidor particular, que a su vez analizará los datos para generar la información para el usuario. En términos comerciales, los sensores también actuarán como recopiladores de datos, la nube será una plataforma para almacenar y analizar los datos, y el *Big Data Analytics* convertirá estos datos en bruto, en conocimiento.

Los modelos de negocio para el empleo del *IoT* pueden variar para cada organización, dependiendo de si está manejando las operaciones básicas, la fabricación, los servicios o tecnologías. Por ejemplo, el sector de la venta al por menor y la mercadotecnia podría beneficiarse de las innovaciones del *IoT* en el futuro: si un nuevo cliente entra a una tienda de zapatos, su tamaño de zapato podría medirse con los sensores de medición. Los datos podrían enviarse a través de la nube sobre la disponibilidad de existencias, el inventario podría reponerse en tiempo real en base al análisis y tendencias pronosticadas. Otros ejemplos para el mismo punto de venta podrían ser los sensores de aparcamiento, de movimiento, ambientales, de puerta que miden las pisadas y los servicios de pago móvil.

La red de personas y cosas



La red de redes es el Internet, lleno de personas y cosas, donde cada conexión máquina-a-máquina se realiza realmente a través de la interacción humana. Estas redes son a la vez redes de colaboración, pero también redes de oposición y amenaza: no hay "dentro" ni "fuera" en este espacio diverso y vulnerable.

47%

Global

de los puestos de trabajo en las economías avanzadas tienen alto riesgo de ser automatizadas en los próximos 20 años.

Transforming talent, the banker of the future: Global banking outlook 2016 - EY

El *IoT* no es nuevo

Aunque el *IoT* es un tema candente hoy en día, no es un concepto nuevo. La frase Internet de las Cosas fue acuñada por Kevin Ashton en 1999. El concepto era relativamente simple, pero poderoso.

"Si tuviéramos computadoras que supieran todo lo que hay que saber acerca de las cosas - utilizando datos que recopilaron sin ninguna ayuda de nosotros - seríamos capaces de rastrear y contar todo, y reducir en gran medida el derroche, la pérdida y el costo. Sabríamos cuándo las cosas necesitan ser reemplazadas, reparadas o mantenidas, y si estas están operativas o deterioradas. El *IoT* tiene el potencial de cambiar el mundo, al igual que lo hizo Internet, y quizá aun más."

Kevin Ashton, "That 'Internet of Things' Thing," RFID Journal, July 22, 1999

Sin embargo, en 1999, todavía habían más preguntas que respuestas a los conceptos del *IoT*:

- ¿Cómo conectamos todo lo que hay en el planeta?
- ¿Qué tipo de comunicaciones inalámbricas podrían ser incorporadas en los dispositivos?
- ¿Qué cambios se necesitarían para soportar billones de nuevos dispositivos en comunicación constante?
- ¿Qué mantiene operativo estos dispositivos?
- ¿Qué debe ser desarrollado para que las soluciones sean rentables?

2015 - tecnologías que permiten el crecimiento exitoso del *IoT*

- El tamaño y el costo de los radios inalámbricos ha disminuido enormemente.
- El Protocolo de Internet versión 6 (*Internet Protocol version 6 - IPv6* por sus siglas en inglés), permite asignar una identificación a las comunicaciones de billones de dispositivos.
- Las compañías electrónicas están incorporando *Wi-Fi* y conectividad inalámbrica celular en una amplia gama de dispositivos (por ejemplo, miles de millones de *chips* inalámbricos).
- La cobertura de datos móviles ha mejorado significativamente con muchas redes que ofrecen velocidades de banda ancha.
- La tecnología de baterías ha mejorado notablemente y la recarga solar se ha incorporado en numerosos dispositivos.

La nube proporciona una plataforma para que el *IoT* prospere; sin embargo, todavía hay muchos desafíos. Con la gran cantidad de datos que mantendrán, los servidores de almacenamiento, tendrán que ser actualizados y protegidos todo el tiempo.

Ahora que hemos entrado en la era de la coordinación de máquina a máquina, de persona a máquina y de persona a persona, las interconexiones se han vuelto mucho más fáciles.

¿Qué oportunidades ofrece el *IoT*?

El *IoT* está liderando el cambio dentro del panorama digital y se está convirtiendo rápidamente en el elemento imprescindible de la tecnología empresarial. Algunas de las principales fuerzas que impulsan la adopción del *IoT* son:

- **Nuevas oportunidades de negocio**
  La red de dispositivos, personas y datos conectados proporcionará oportunidades de negocio a muchos sectores. Las organizaciones podrán utilizar los datos del *IoT* para comprender mejor las necesidades de sus clientes y mejorar los procesos, así como la coordinación de la cadena de suministro o inventario, las inversiones y la seguridad pública.
- **Potencial para el crecimiento de los ingresos empresariales**
  Existen múltiples oportunidades de impacto económico sin explotar al encontrar formas creativas de implementar la tecnología del *IoT* e impulsar el crecimiento de los ingresos y la creación de valor de primera línea; a través de la reducción de gastos y la mejora de la productividad de los activos.
- **Mejora en la toma de decisiones**
  Los dispositivos inteligentes de computación personal están en alza, lo que lleva a opciones más amplias, actualizaciones en tiempo real, instalaciones mejoradas, información más precisa, entre otros; y así lograr una toma de decisiones más informada.
- **Reducción de costos**
  Los costos de los componentes del *IoT* como los servicios en la nube, los sensores, los dispositivos *GPS* y los *microchips*, han disminuido; lo que significa que el costo de los dispositivos conectados al *IoT* es cada día más asequible.
- **Seguridad y protección**
  Con la ayuda de cámaras y sensores, existe la posibilidad de protegerse y evitar amenazas físicas que puedan ocurrir en el lugar de trabajo o en el hogar. Con el tiempo, incluso la gestión de desastres o los sistemas de recuperación, obtendrán ayuda del *IoT*.

- **Mejor experiencia ciudadana**
  La experiencia ciudadana podría mejorar considerablemente debido a la facilidad de acceso y de comunicación. Piense, por ejemplo, en que un ciudadano pueda pagar sus impuestos a distancia, ver su espacio de estacionamiento desde la oficina, apagar o comunicarse con aparatos o dispositivos en el hogar, e incluso, de manera proactiva, controlar su salud.

- **Infraestructura mejorada**
  El *IoT* podría ayudar a convertir la infraestructura en un organismo vivo, especialmente cuando las grandes mega ciudades se transforman en ciudades inteligentes. La población en las zonas urbanas y las escasas fuentes de energía no renovables, dificultan la gestión de los recursos; pero la infraestructura inteligente y las redes interconectadas, están comenzando a proporcionar soluciones con aspectos tales como redes inteligentes, gestión inteligente de residuos, control inteligente de tráfico, servicios públicos inteligentes y ciudad sostenible. Los servicios de ciudadanía automatizados habilitados para microcomputadoras también harán que las futuras ciudades inteligentes sean más seguras y eficientes.

70%

Global

de los dispositivos más utilizados del IoT son vulnerables a sufrir algún tipo de ataque cibernético.

Internet of Things, research study 2015 - HP Enterprise

El mundo del *IoT* en constante expansión

El *IoT* ya está integrado en varias áreas donde la adopción de tecnología se está acelerando. Las áreas clave líderes en la integración del *IoT* son:

Vida inteligente

Una tecnología innovadora y de vanguardia apunta a hacer la vida más sencilla y segura para el consumidor. Una vida inteligente incluye:

- **Atención de salud** - un nuevo modelo centrado en el paciente está emergiendo
- **Empresas de consumo y minoristas** - la edad de los clientes empoderados y co-creadores
- **Convergencia bancaria** - nuevos modelos para la banca y las finanzas
- **Seguros** - pasando de estadísticas a políticas basadas en hechos individuales
- **Servicios públicos** - eficiencia y conveniencia de conducción para los gobiernos y los ciudadanos

Movilidad inteligente

La gestión en tiempo real y las soluciones de rutas tienen como objetivo hacer que los viajes sean más agradables y el transporte más confiable. Una movilidad inteligente incluye:

- **Conducción autónoma y un auto interconectado**
- **Movilidad urbana** - gestión inteligente del tráfico
- **Movilidad interurbana** - conexión a través de las redes de transporte
- **Gestión de tarifas y soluciones de pago**
- **Distribución y logística**
- **Gestión de flotas**

Ciudad inteligente

Las innovaciones tendrán como objetivo mejorar la calidad de vida en las ciudades, abarcando cuestiones de seguridad y recursos energéticos. Una ciudad inteligente incluye:

- **Gestión más inteligente de la infraestructura de la ciudad** - utilizando *Big Data Analytics*
- **Colaboración entre múltiples agencias** - utilizando tecnologías en la nube
- **Recopilación de datos en tiempo real, que permita una respuesta rápida** - utilizando tecnologías móviles
- **Mayor seguridad** - mejor seguridad pública y aplicación de la ley, y respuesta más eficiente ante emergencias
- **Mejora de la planificación de la ciudad** – mejoras en los esquemas, gestión de proyectos y entrega de resultados
- **Utilidades en red** - medición inteligente y gestión de la red
- **Desarrollos de edificios** - más automatización y mejor gestión y seguridad

Fabricación inteligente

Las soluciones de fábrica y logísticas se crearán específicamente para optimizar procesos, controles y calidad. Una fabricación inteligente incluye:

- **Aprendizaje de máquinas** - toma de decisiones inteligentes y automatizadas
- **Comunicaciones de maquinaria** - más interacción y colaboración
- **Redes** - control y gestión en red de equipos de fabricación
- **Procesos optimizados** - prototipaje y fabricación rápida, procesos mejorados y operaciones más eficientes de la cadena de suministro
- **Gestión preventiva de activos** - mediante diagnósticos preventivos y mantenimiento
- **Mejora de integración de infraestructuras** - superar el problema de ausencia de estándares de interfaz

Beneficios económicos del *IoT*

Al igual que cualquier otro mercado donde la demanda es directamente proporcional al suministro, el *IoT* también tiene una economía con el potencial de crear miles de millones de dólares de valor, tanto para los usuarios finales, como para las empresas del sector público y privado.

Con el crecimiento del *IoT*, muchas tecnologías de TI crecerán en paralelo. Por ejemplo, la computación en la nube y los mercados de *Big Data* le dan al *IoT* una plataforma donde crecer y evolucionar.

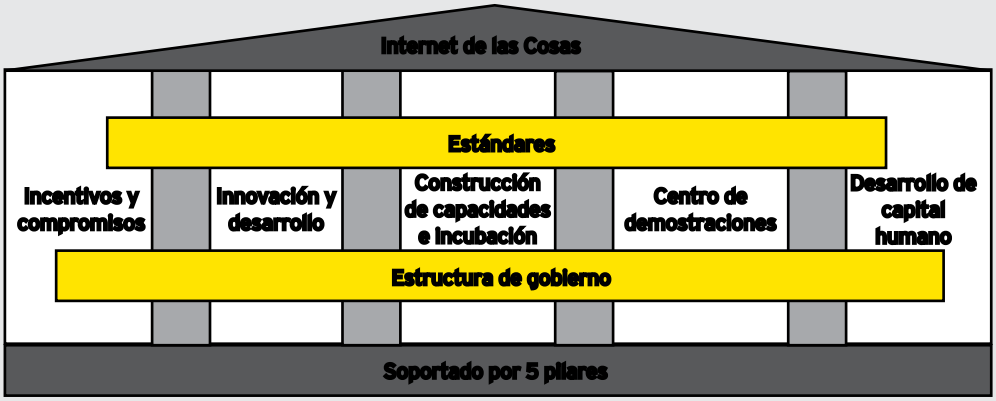
El *IoT* ofrecerá oportunidades a empresas que fabrican bienes del *IoT*, así como a aquellas empresas que prestan servicios relacionados con el *IoT*. Los fabricantes de dispositivos inteligentes, sensores, o solenoides (activadores); asi como los desarrolladores de aplicaciones, estrategas de marketing, compañías analíticas y proveedores de servicios de Internet, todos se beneficiarán por la evolución del *IoT*. Según las estimaciones de la industria, las comunicaciones de máquina a máquina por sí solas generarán aproximadamente US$ 900 mil millones en ingresos al 2020.

El mercado se está centrando actualmente en los dominios verticales del *IoT* ya que se encuentra en fases relativamente tempranas de desarrollo. Pero el *IoT* no puede ser tratado como una plataforma única, o como una sola tecnología. Con el fin de lograr el rápido crecimiento esperado de las oportunidades del *IoT*, se debe poner más énfasis en las interfaces, plataformas, aplicaciones móviles y estándares comunes o dominantes.

Marco de políticas del *IoT*: perspectiva de las economías en desarrollo

India planea invertir aproximadamente US$ 11 mil millones para desarrollar 100 ciudades inteligentes. En octubre de 2014, el gobierno de la India publicó un proyecto de documento marco de política del *IoT*, que propuso el siguiente modelo:

Los dos pilares horizontales son los estándares y la estructura de gobierno, que se definen como las dos fuerzas gobernantes. Se puede decir que el futuro del *IoT* depende de estos dos, ya que los primeros definirán los estándares de comunicación, seguridad y privacidad; mientras que los segundos definirán la formación, el control y el poder de las agencias gubernamentales.



Fuente: Departamento de Electrónica y Tecnología de la Información, Gobierno de la India

El *IoT* afectará a los diversos sectores empresariales de diferentes maneras

Los sectores clave, como salud, educación, financiero, comercio minorista, comunicaciones, hotelería, industria, transporte y agricultura, ya están enriquecidos por la tecnología basada en Internet y otros avances, los cuales permitirán que otros sectores económicos clave formen parte de la conectividad digital.

En la última década, el **sector salud** ha sido uno de los mayores beneficiarios del *IoT*. Las soluciones futuras pueden estar disponibles como:

- Información personal que podría detallar a los médicos, no sólo sobre la historia clínica de las personas, sino también sobre sus enfermedades potenciales.
- Sensores y microcomputadoras ubicadas en el cuerpo humano que pudieran monitorear las condiciones de salud e incluso avisar a los servicios de emergencia en caso de algún problema.
    - Una tecnología similar podría hacer que el ambiente de vida sea más adecuado para los requisitos médicos de una persona.
- Los dispositivos y procesos altamente automatizados podrían ayudar a aumentar la eficacia de los tratamientos críticos con una interfaz humana limitada.

El *IoT* en el **sector educación** ya ha comenzado a automatizar el sistema convencional: las aulas inteligentes interactivas están ayudando a los estudiantes a aprender y participar más, mientras que la asistencia automática y varios sistemas de seguimiento de los estudiantes podrían ayudar a hacer las escuelas más seguras. Las aulas remotas habilitadas para Internet serán un hito para los países en desarrollo, penetrando profundamente en áreas donde no es posible establecer una infraestructura escolar tradicional.

Las **unidades industriales y de fabricación** habilitadas para Internet, están dando resultados diferenciadores, haciéndolos más seguros y eficientes a través de controles automatizados de procesos. La optimización de las plantas y la energía, el control de la salud y la gestión de la seguridad son cada vez más controlados por sensores avanzados, conectados en red a través de sofisticados microordenadores.

Los **servicios financieros** ya están aprovechando el Internet para muchos de sus servicios. La mejora exponencial de la infraestructura digital y la próxima generación de productos habilitados para el *IoT* podrían liderar aún más el crecimiento del sector financiero, con innovaciones como dispositivos de monitoreo *smart wearable*, ayudando a los clientes a rastrear mejor su dinero e inversiones.

Las **empresas de telecomunicaciones** podrían enfrentar un aumento en el uso de datos debido a los dispositivos habilitados para el *IoT*, lo que elevaría su ingreso promedio por usuario (*Average Revenue Per User - ARPU* por sus siglas en inglés); mientras que por otro lado, también tendrán que lidiar con algunas preocupaciones, como la privacidad y la seguridad de su infraestructura.

Según las estimaciones de la industria, las comunicaciones de máquina a máquina, por sí solas, generarán aproximadamente 900,000 millones de dólares en ingresos para 2020.

Enfoque

El auto interconectado

El auto interconectado es sólo una de las maneras en que el *IoT* va a impactar nuestras vidas significativamente (y muy visiblemente) en un futuro próximo. Aquí abordamos los requisitos de seguridad de la plataforma de autos interconectados y su entorno, pero el enfoque es relevante para todas las innovaciones relacionadas con el *IoT*.

Seguridad del auto interconectado

De forma similar a otros sistemas móviles y conectados a Internet, el ecosistema del auto interconectado debe ser visto como una "red de redes" (o un sistema de sistemas). El auto interconectado es sólo un enlace más (aunque el más nuevo y de mayor foco de atención) en una red mucho más amplia y compleja.

Al tomar este punto de vista, vemos la necesidad de desplazar el énfasis del auto interconectado como un sistema limpio, con límites claros y puntos de entrada o salida, y tomar como objeto de protección a las propias redes, es decir, las interacciones entre los usuarios o propietarios de los vehículos y los numerosos otros actores en el ecosistema. La seguridad se convierte entonces en la seguridad de esas interacciones y no se limita al auto como un ente aislado.

Es vital comprender el carácter desigual de las tecnologías digitales y de red. Así, por ejemplo, mientras que algunos estudios predicen que el 70-90% de los vehículos de motor podrán estar conectados en el año 2020, otros datos indican que el 80% de esta conectividad será muy limitada (por ejemplo, sólo a través del teléfono móvil y sólo para entretenimiento y servicios de contenido). No habrá conexiones universales entre marcas y mucho menos para toda la funcionalidad de los nuevos autos en el futuro próximo.

Cambio fundamental

Debido a que el auto interconectado "vive" en la red, la seguridad no es una cuestión de cerrar puertas y cifrar datos. Seguridad significa gestionar datos compartidos y una red de participantes más compleja. La apertura de Internet significa que las redes y aplicaciones heredadas quedan expuestas y el "área de ataque" aumenta a medida que el modelo de negocio se expande a nuevas áreas, socios y tipos de usuarios.

La red de redes se convierte en el objetivo de la protección y la seguridad, y no el auto como ente individual, y todas las medidas y tecnologías de seguridad cibernética deben alinearse con este objetivo en mente. Los requisitos de seguridad deben ser abordados a nivel de aplicación o canal, pero en algunos casos, esto bloquea la capacidad del fabricante de autos para tener una estrategia viable y coherente.

Al considerar las iniciativas de autos interconectados, las empresas deben establecer una sólida comprensión jurídica de las políticas de protección de datos. Sólo sobre esta base será posible diseñar y mejorar servicios seguros que mejorarán las operaciones comerciales. Hasta ahora, en Europa y el resto del mundo, las cuestiones relativas a la protección de datos todavía no tienen una respuesta uniforme y esta área requiere más trabajo desde el punto de vista de la seguridad de la información.

Las redes de autos interconectados necesitan medidas de protección estándar como *gateways* de seguridad y *firewalls* (para bloquear ataques), pero esto también requiere varias capas o zonas (basadas en niveles de aseguramiento y controles de acceso) donde cada capa implementa una política de seguridad. La propiedad y la clasificación de datos deben sostener los niveles de seguridad (rutas y roles de acceso separados, etc.).

La conexión a múltiples redes confiables y no confiables requiere un nuevo modelo de confianza, pero cerrando la brecha de confianza entre el fabricante y el propietario del automóvil y entre el fabricante y los socios comerciales (proveedores) significa equilibrar el riesgo y las consideraciones de confianza para crear una situación beneficiosa para todos.

El mercado de postventa y el desarrollo de relaciones comerciales pueden ser facilitados por un modelo de seguridad con claras reglas de participación y de intercambio de datos, por ejemplo:

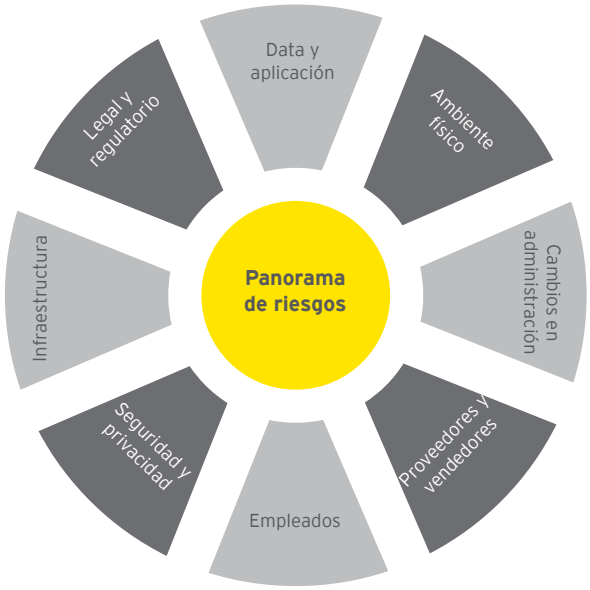
- Nuevas funciones que estén siendo adoptadas por la empresa (por ejemplo, operando de forma incremental en varias funciones, inclusive como proveedores de servicios)
- El negocio opera en una "cadena de valor" extendida sin fronteras
- Se introducen nuevos socios (proveedores de contenidos, etc.)
- Crea nuevas relaciones con los clientes (por ejemplo, permitir a los clientes seleccionar productos y servicios en línea)
- Ampliación de las redes y tecnologías de información (por ejemplo, vinculación de redes de transporte y distribución, o establecimiento de conexiones con vehículos para fines de servicio, mantenimiento y comercialización)
- Vincular sistemas previamente aislados físicamente bajo redes de colaboración y habilitar el acceso remoto (por ejemplo, escritorios virtuales y *software* como servicio)

El incremento de la amenaza cibernética

Mientras que el *IoT* está ingresando diariamente en nuestras vidas, cada vez hay más riesgos de seguridad pertenecientes al *IoT* y estos van cambiando rápidamente. En el mundo de hoy, de tecnología siempre conectada y sin suficiente consciencia de seguridad de parte de los usuarios, los ataques cibernéticos ya no son una cuestión de "si nos ocurrirá" sino más bien de "cuándo nos ocurrirá".

Los criminales cibernéticos están trabajando en técnicas para evadir la seguridad de las organizaciones, accediendo a todo, desde información de propiedad intelectual hasta la información individual del consumidor. Hacen esto para causar daño, irrumpir data sensible y robar propiedad intelectual.

Todos los días, sus ataques se vuelven más sofisticados y más difíciles de vencer. A consecuencia de este desarrollo continuo, no podemos descifrar con exactitud qué tipo de amenazas emergerán el próximo año, en cinco o en diez años; sólo podemos decir que estas amenazas serán más peligrosas que las del presente. También podemos afirmar con certeza que mientras las fuentes antiguas de esta amenaza se desvanecen, nuevas fuentes emergerán para tomar su lugar. A pesar de esta incertidumbre – es más, gracias a ella – tenemos que ser claros con respecto al tipo de control de seguridad requerido.



70%

Global

de los dispositivos del IoT más comúnmente usados tienen vulnerabilidades.

HP study reveals 70% of Internet of Things devices vulnerable to attack. (s.f.) Obtenido de http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VHMpw4uUfVc

55%
Global

97%
Perú

no tiene o sólo tiene una capacidad informal de identificación de vulnerabilidad.

La seguridad cibernética efectiva es cada vez más difícil de alcanzar. El perímetro organizacional tradicional se está erosionando y las defensas de seguridad existentes están bajo una creciente presión. Las soluciones puntuales, en particular el antivirus, sistema de detección de intrusiones (*Intrusion Detection System - IDS* de sus siglas en inglés), *IPS*, parches y cifrado, siguen siendo un control clave para combatir los ataques conocidos de hoy en día. Sin embargo, se vuelven menos eficaces con el tiempo a medida que los *hackers* encuentran nuevas maneras de evadir los controles.

Los ataques cibernéticos han transformado el panorama de riesgos

Es importante recordar que la seguridad cibernética es un problema a nivel de todo el negocio, no sólo un riesgo tecnológico. Debido a que muchas oportunidades para el *IoT* surgirán a través de la integración y colaboración tecnológica, que continuará incrementando su complejidad – esta complejidad genera mayores escenarios de riesgo.

Los modelos probados de manejo de riesgos tradicionales tienen sus orígenes y sabiduría todavía enfocados en un mundo en el cual la organización es dueña y posee la mayoría, si no son todos, de los activos de datos que fluyen a través de los sistemas. El mayor uso de Internet y del trabajo móvil significa que los límites de la empresa están desapareciendo y como resultado, el panorama de riesgo también se vuelve ilimitado.

Dado que la mayoría de los negocios hoy en día se hacen fuera de la valla defensiva de las organizaciones, es vital para las misma que sean capaces de comunicarse con sus socios de negocios, y para hacer esto tienen que crear huecos en dicha valla. Como resultado, un sistema de seguridad cibernética también debe incluir las redes más amplias de la organización, incluyendo clientes, consumidores, proveedores, vendedores, colaboradores, socios e incluso antiguos alumnos; en conjunto llamados ecosistema de negocios.

Un enfoque estándar en la administración de riesgos asume que el límite de confianza ya está definido. Lo que falta en el enfoque centrado en los riesgos y en lo tecno-céntrico es todo lo relacionado con la gestión de la confianza, es decir, las nuevas funciones y procesos y las nuevas políticas y estructuras necesarias para ampliar esta frontera del riesgo.

Un ecosistema extendido es gobernado y administrado por varios actores con políticas y requerimientos de seguridad individuales; y estos actores, en ocasiones, tienen intereses y objetivos de negocios muy diferentes. Por lo tanto, es necesario ajustar el enfoque tradicional de riesgo de la compañía para tomar esto en consideración estos nuevos aspectos.

Para que una organización pueda manejar el riesgo en el ecosistema de manera efectiva, necesita definir claramente los límites de dicho ecosistema. También necesita decidir qué está dispuesta a manejar dentro de estos límites: ¿será solamente el riesgo que enfrentan los grupos que están a un paso de la organización misma (por ejemplo: proveedores) o debería la organización también intentar influenciar la mitigación de riesgos que enfrentan grupos que están a dos pasos del centro (por ejemplo: proveedores de los proveedores)?

La seguridad del dispositivo sólo es tan segura como la red en la cual reside: esto incluye a las personas, procesos y tecnologías involucradas en el desarrollo y entrega.

El efecto multiplicador de los desafíos de la seguridad cibernética hoy en día

La interconectividad de las personas, dispositivos y organizaciones en el mundo digital de hoy, despliega un nuevo campo de vulnerabilidades por los cuales los criminales cibernéticos pueden entrar. El paisaje global del riesgo de la organización es sólo una parte de un universo potencialmente contradictorio de amenazas reales y potenciales que con demasiada frecuencia vienen de actores de amenazas completamente inesperadas, lo que puede tener un efecto creciente.

La rapidez del cambio

En este mundo post crisis económica, los negocios se mueven rápido. Nuevos productos son lanzados, fusiones, adquisiciones, expansión del mercado y la introducción de nuevas tecnologías están en aumento: estos cambios tienen invariablemente un impacto complicado en la fuerza y amplitud de la seguridad cibernética de una organización y su capacidad para mantener el ritmo.

Una red de redes

La adopción de la informática móvil ha dado lugar a una confusión en divisar los límites de la organización, con TI acercándose al usuario y alejándose de la organización. El uso de Internet a través de *smartphones* y *tablets* (en combinación con estrategias de *Bring Your Own Device* – "traer su propio dispositivo" - por parte de los empleadores) ha hecho que los datos de una organización sean accesibles en cualquier lugar y en cualquier momento.

Inevitablemente, un dispositivo vulnerable puede conducir a otros dispositivos vulnerables, y es casi imposible parchar todas las vulnerabilidades de todos los dispositivos. Para los delincuentes cibernéticos, no será difícil encontrar un objetivo para su ataque. El mercado de la vulnerabilidad (el mercado negro subterráneo que vende *botnets, zero days, rootkits,* etc.) será muy amplio al igual que el número de víctimas. Es más fácil para un atacante plantar un "troyano" en un teléfono, si el teléfono se encuentra conectado a una computadora que ya ha sido comprometida. Con aún más dispositivos conectados, será aún más fácil para un criminal cibernético entrar en su vector de ataque.

Las máquinas o dispositivos ayudarán a las personas a realizar la mayoría de sus tareas, pero consideren el escenario en el cual alguien pueda echar un vistazo a cualquiera de nuestros dispositivos inteligentes. En eventos recientes, los *hackers* accedieron a un monitor de bebé y después de definir su punto de entrada y de salida, ingresaron a la casa.

Infraestructura

Encontrar brechas para entrar a una red será más fácil para cualquier atacante debido a que habrá muchas maneras de atacar. A los sistemas de tecnología de operatividad cerrada tradicionales se les ha otorgado cada vez más direcciones *IP* desde las cuales se puede acceder externamente, así que las amenazas cibernéticas se están abriendo camino desde los sistemas de *backoffice* hacia las infraestructuras críticas, como los sistemas de generación de energía y sistemas de transporte, entre otros sistemas automatizados.

Computación en la nube

La computación en la nube ha sido un pre-requisito para el *IoT* desde los primeros días de su evolución. La nube proporciona una plataforma para que el *IoT* florezca; sin embargo, todavía hay muchos desafíos que enfrentamos hoy en día cuando se trata de la seguridad en la nube o la seguridad de datos en la nube. Las organizaciones a menudo descubren demasiado tarde que los estándares de seguridad de su proveedor de servicios en la nube pueden no corresponder a los suyos. Los recientes acontecimientos de *CelebGate* y la manera en la que fueron comprometidas las infraestructuras como servicios (*Infrastructure as a Service - IAAS* por sus siglas en inglés) de Amazon son ejemplos vivos de tales defectos. Estos son los incidentes que han llevado a los críticos a llamar a estos servicios como un punto único de *hackeo*, en lugar de un punto único de almacenamiento.

Con *Big Data* también entrando en el panorama, habrá una enorme cantidad de datos producidos también para los proveedores de servicios. Con la gran cantidad de datos que ellos tendrán, los servidores de almacenamiento tendrán que estar actualizados y protegidos todo el tiempo. También habrá un aumento en los riesgos de los enlaces de comunicación, ya que los sensores y dispositivos estarán comunicando información personal sensible todo el tiempo en dichos canales.

Con nuestros datos almacenados en dichos servicios en la nube, existe también el riesgo de que aumenten los mensajes de *spam*, ya que los servidores de la nube se trasladan prácticamente de una ubicación geográfica a otra en cuestión de minutos. Por lo tanto, no hay bloqueo específico de *IP* posible para ningún *spam*.

Riesgo en la aplicación

Las aplicaciones han acelerado la integración de dispositivos móviles en nuestra vida diaria. Desde aplicaciones de mapeo, redes sociales, herramientas de productividad, a juegos, las aplicaciones han conducido grandemente la revolución de los teléfonos inteligentes y la han hecho tan significativa y amplia como lo es hoy en día. Mientras que, las aplicaciones demuestran una utilidad que aparentemente sólo está vinculada por la imaginación del desarrollador, también incrementa el riesgo de ser compatibles con dispositivos *Bring Your Own Device* (*BYOD*) en un ambiente corporativo.

Mientras la organización permite a los empleados llevar sus propios dispositivos, inevitablemente se presenta la necesidad de usar esos mismos dispositivos para acceder información relacionada con el trabajo. Esto presenta principalmente dos riesgos de seguridad:

- Aplicaciones maliciosas (*malware*): el aumento del número de aplicaciones en el dispositivo incrementa la probabilidad de que algunas puedan contener código malicioso o brechas de seguridad
- Vulnerabilidades de aplicaciones: aplicaciones desarrolladas o desplegadas por la organización para permitir el acceso a información corporativa pueden contener debilidades de seguridad

253
mil
millones

Global

El número estimado de aplicaciones gratis está proyectado a llegar a 253 mil millones para el 2017.

Obtenido de
http://www.statista.com/statistics/241587/number-of-free-mobile-app-downloads-worldwide

Creciente uso de dispositivos móviles

Los teléfonos inteligentes ya se han convertido en una parte integral de nuestras vidas. Nos fiamos de ellos para mantener información importante, como nuestra dirección de domicilio, detalles de la tarjeta de crédito, fotos y videos personales, cuentas de correo electrónico, documentos oficiales, números de contacto y mensajes. La información almacenada en nuestros dispositivos incluirá los lugares que visitamos con frecuencia y un patrón que nos identifica de manera única, por lo que cualquier persona que pueda *hackear* alguno de estos dispositivos puede entrar en nuestras vidas muy fácilmente.

La pérdida de un solo dispositivo inteligente no significa únicamente la pérdida de información, sino que, de manera creciente, también conduce a una pérdida de identidad (robo de identidad). En Internet no hay monopolio por lo que todos los dispositivos no tienen el mismo *firmware* o *software*. *Hardware* de diferentes compañías podrían no ser compatibles entre sí y, por lo tanto, podrían conducir a problemas de interoperabilidad de los dispositivos.

El aumento en el número de dispositivos también puede ser un problema ya que las vulnerabilidades con las que se asocian se extenderán muy rápidamente. Con miles de vendedores alrededor del mundo, será muy difícil para los ingenieros de red corregir estas vulnerabilidades, especialmente con miles de nuevas correcciones para actualizar diariamente - ingenieros de red del *IoT* ahora tendrá diez veces la cantidad de dispositivos comunicándose a sus servidores fuera de la red.

Los delincuentes cibernéticos organizados podrán vender *hardware* con troyanos o *back doors* ya instalados en ellos, y con la ayuda de estas vulnerabilidades, van a buscar a otras víctimas y hacer con ellos una red de ataque. Estos dispositivos, repartidos por todo el mundo, serán perfectos para un ataque de denegación de servicio distribuido (*Distributed Denial of Service - DDoS* por sus siglas en inglés) en cualquiera de los servidores, ya que los sensores no tienen antivirus.

El empleador *Bring Your Own Device* (*BYOD*)

Con la mayoría de los empleados ahora poseedores de dispositivos móviles, las organizaciones han estado explotando el hecho de que sus empleados, cada vez más, quieren utilizar sus propios dispositivos móviles personales para llevar a cabo el trabajo (a menudo junto con los dispositivos proporcionados por las empresas), o si una organización requiere que sus empleados lo hagan, es una alternativa más barata que proporcionar los dispositivos propios de la organización. Muchas organizaciones están acudiendo a la TI corporativa para apoyar esto.

Sin embargo, *BYOD* tiene un impacto significativo en el modelo de seguridad tradicional de proteger el perímetro de la organización de TI, difuminando la definición de ese perímetro, tanto en términos de ubicación física como de propiedad de activos. Debe utilizarse un enfoque holístico y metódico para definir este riesgo y ayudar a garantizar que existen controles para mantener la seguridad y la facilidad de uso de los dispositivos en la empresa.

Consumo de ancho de banda

Miles de sensores, tratando de comunicarse con un solo servidor, crearán una saturación del tráfico de datos que podría traer abajo el servidor. Además, la mayoría de los sensores usan un enlace sin cifrar para comunicarse, y por lo tanto, existe la posibilidad de una brecha en la seguridad.

El consumo de ancho de banda de miles de millones de dispositivos pondrá tensión en el espectro de otras comunicaciones inalámbricas, que también operan en las frecuencias de megahertz como la radio, televisión, servicios de emergencia, etc. Sin embargo, las empresas han comenzado a tomar esto en serio; como resultado, Qualcomm ha lanzado su plataforma de conectividad *Wi-Fi* de bajo consumo para el *IoT*.

Cuestiones de gobernanza y cumplimiento

El incremento de legislación de privacidad es una tendencia que probablemente continuará en el futuro cercano. A medida que las organizaciones diseñan controles de seguridad del *IoT*, estos pueden interferir con las expectativas personales de privacidad. Una política del *IoT* bien formada debe incluir expectativas claras y definidas sobre los procedimientos que afectan la privacidad, teniendo en cuenta que la legislación puede diferir en ciertas regiones geográficas.

Protección de privacidad e información

Todos los dispositivos inteligentes contienen información sobre sus usuarios, que van desde su plan de dieta hasta donde trabajan detalles personales de vida y a menudo incluso detalles bancarios. Todos los dispositivos del *IoT* recopilan datos precisos del mundo real, que es muy bueno desde una perspectiva analítica, pero algún usuario podría no estar cómodo compartiendo esa información con un tercero, así toda esta información no sea confidencial o sensible.

Con el exceso de datos de miles de millones de dispositivos, habrá muchas oportunidades para las organizaciones analíticas. Estos marcos analíticos serán capaces de cuantificar el ambiente empresarial alrededor de los usuarios, pero al mismo tiempo, la puesta en valor de estos datos puede conducir a problemas de privacidad. La pregunta es: ¿nos sentimos cómodos al compartir nuestros datos con personas de las que ni siquiera somos conscientes? ¿no se siente como una brecha en nuestra privacidad? ¿debería haber una mayor transparencia sobre cómo se almacenan, utilizan y transportan los datos?

De acuerdo con *OWASP* (*Open Source Web Application Security Project* - proyecto de seguridad de aplicaciones web de código abierto), algunos de los principales riesgos de privacidad también contienen vulnerabilidades de aplicación web, fugas de datos del lado del operador, respuesta insuficiente ante vulneración de datos, intercambio de datos con terceros y transferencia insegura de datos.

En la aplicación de la legislación sobre protección y privacidad de datos, así como del modelo de control de acceso, uno de los principales objetivos es que los datos añadidos de los clientes no permitan usos anticompetitivos, ilegales o discriminatorios. La recopilación de información personal debe estar siempre formalmente justificada (incluida una evaluación de impacto) y restringida al mínimo necesario para fines comerciales. De acuerdo con las regulaciones establecidas, los datos deben ser retenidos por el menor tiempo posible, estrictamente para apoyar las operaciones comerciales.

Si la organización está recopilando datos personales, el propósito, vencimiento, seguridad, etc., de los datos recopilados debe estar claramente establecido en la política de seguridad de la información. La organización también debe realizar una evaluación de los riesgos asociados con el procesamiento.

Si los datos son procesados por un tercero (es decir, si la organización utiliza un proveedor de correo electrónico en la nube), es importante que los datos estén protegidos por un acuerdo de procesamiento de datos con el tercero. Con la transferencia de datos, la responsabilidad de proteger esos datos también debe ser transferida y el cumplimiento verificado de manera periódica. Sin embargo, es interesante observar que la mayoría de los proveedores de la nube actualmente no tienen una política de privacidad o tienen políticas no transparentes, lo que hace que los usuarios se sientan un poco incómodos al acudir a ellos.

Investigación y notificación de infracción

Tras la repercusión de los ataques cibernéticos altamente divulgados por los medios de comunicación, se propone una nueva y futura legislación sobre seguridad cibernética, con multas siendo impuestas a empresas que no protegen los datos de los consumidores y se están introduciendo medidas obligatorias en torno a la notificación ante la infracción de datos. Las organizaciones deben prepararse para esta legislación manteniendo un inventario vigente de los dispositivos, los datos sobre ellos y los controles de seguridad colocados para proteger esos datos.

Algunos de los principales riesgos de privacidad son las vulnerabilidades de las aplicaciones *web*, las fugas de datos del lado del operador, la insuficiente respuesta ante la infracción de datos, el intercambio de datos con terceros y la transferencia insegura de datos.*

**OWASP, Top 10 Privacy Risks Project. (s.f.) Obtenido de https://www.owasp.org/index. php/OWASP_Top_10_Privacy_Risks_Project*

Enfoque

Seguridad cibernética y redes inteligentes de energía

Un cambio radical en la evolución del ecosistema de la energía

Los medidores inteligentes y las infraestructuras de red generarán beneficios considerables a lo largo del ciclo de vida de la energía, desde la generación hasta la distribución y el consumo. Esto incluye:

- La capacidad de igualar la oferta y la demanda
- Reducción de costos a través de la administración remota de dispositivos
- Consumidores mejor informados a través de la disponibilidad en tiempo real de datos de consumo de energía granular

Sin embargo, si la transición hacia una gestión inteligente de la energía de la red no se desarrolla correctamente, existen amenazas significativas de seguridad cibernética a las que las organizaciones que operan en este espacio estarán expuestas.

Medidor inteligente y complejidad de la red inteligente

La infraestructura del medidor inteligente depende de un amplio conjunto de sistemas en red, con diferentes tecnologías y niveles de seguridad, creando un entorno que es difícil de evaluar desde el punto de vista de la protección de datos y la gestión de amenazas cibernéticas.

Las redes empresariales de proveedores de energía, cada una con su propio ecosistema, deben estar conectadas a los medidores inteligentes y a la infraestructura de red, generando requisitos para la estandarización y regulación de los mecanismos y procesos de seguridad. La complejidad de este entorno no es comprensible para el público en general.

El uso legítimo de los datos almacenados debe complementarse con mecanismos para minimizar el riesgo de acceso no autorizado, incluida la comercialización ilegal de datos y los reglamentos de retención de datos que abarcan los datos transferidos más allá del proveedor de servicios original.

A nivel técnico, la infraestructura de red y de los medidores inteligentes aparece como una red de redes, regida por asociaciones y organizaciones impulsadas por el mercado, con un importante aporte y regulación del gobierno. Estas asociaciones gestionan o gestionarán grandes cantidades de datos de consumo y operativos, lo que exige un gran esfuerzo en dirección de una estrategia de seguridad colaborativa con funciones específicas y un enfoque conjunto para prevenir y rechazar los ataques cibernéticos.

Enfoque integral de seguridad

Se requiere un enfoque múltiple y de defensa en profundidad para garantizar la seguridad general del sistema de medición inteligente. La solución de seguridad debe tener como objetivo proteger el sistema contra ataques conocidos y desconocidos (ataques de día cero), acceso no autorizado, manipulación física, compromiso de información, negación de servicio, espionaje y otras amenazas.

Se debe implementar un conjunto de controles preventivos, de detección y correctivos para asegurar la seguridad del sistema de medición inteligente, que incluye dispositivos finales, sistemas de administración y monitoreo, infraestructura de red y entornos de pago. Algunos de los controles clave necesarios para cumplir con los requisitos de seguridad de los medidores inteligentes son: segregación de red, cifrado de datos (en tránsito y reposo), monitoreo en tiempo real, solución de autenticación de dispositivo o usuario, registro y cancelación de registro de dispositivos, etc.

El entorno de control debe estar respaldado por un marco de gobernanza, políticas y procedimientos apropiados, monitoreo continuo y un modelo de madurez para asegurar que el sistema de medición inteligente global esté protegido contra problemas conocidos y desconocidos, y responda eficazmente al cambiante panorama de amenazas.

La privacidad y seguridad de los datos de los clientes son fundamentales para asegurar la adopción de medidores inteligentes por parte de los clientes y la esperada reducción de la huella de carbono. Los principios de privacidad por diseño y seguridad por diseño son necesarios para la implementación de la seguridad y privacidad, y los esfuerzos en esta área deben ser bien comprendidos, documentados y visibles para apoyar en la credibilidad de la solución.

Es importante resaltar -como hicimos en el contexto del auto interconectado- que no se ha resuelto toda la cuestión de la protección de datos de los consumidores y los ciudadanos. Existen grandes diferencias en la legislación entre países y regiones, y las empresas se enfrentan a la falta de normas técnicas o industriales universalmente aceptadas.

Una solución segura sólo podría lograrse mediante una visión holística del sistema de medición inteligente y un enfoque estructurado de la gestión de riesgos. Pero para que sea verdaderamente exitoso, la seguridad debe estar incluida en la solución inicial y no ser vista como un "complemento".

Entonces, ¿cómo pueden las organizaciones adelantarse al crimen cibernético?

Es posible que su organización ya tenga fuertes políticas, procesos y tecnologías de TI, pero, ¿está preparada para lo que viene? La alerta temprana y la detección de infracciones son decisivas para estar en estado de preparación, lo que significa que el énfasis de la seguridad cibernética ha cambiado a inteligencia de amenazas. La mayoría de las organizaciones ya saben que existen amenazas para su información y sistemas operativos, así como para sus productos. El paso más allá es entender la naturaleza de esas amenazas y cómo se manifiestan.

Una organización en un estado de preparación para hacer frente a los ataques cibernéticos habita en una mentalidad completamente diferente, ve al mundo de manera diferente y responde de una manera que los delincuentes cibernéticos no esperan. Requiere comportamientos reflexivos, considerados y colaborativos. Aprende, prepara y ensaya. Ninguna organización o gobierno puede predecir o prevenir todos (o incluso la mayoría) de los ataques; pero pueden reducir su atractivo como objetivo, aumentar su resiliencia y limitar el daño de cualquier ataque dado.

Un estado de preparación incluye:

- Diseñar e implementar una estrategia de inteligencia de amenazas cibernéticas para apoyar decisiones empresariales estratégicas y aprovechar el valor de la seguridad
- Definir y abarcar el ecosistema extendido de seguridad cibernética de las organizaciones, incluyendo socios, proveedores, servicios y redes empresariales
- Adoptar un enfoque cibernético, entender sus activos vitales y su valor e invertir específicamente en su protección
- Uso de análisis de datos forenses e inteligencia de amenazas cibernéticas para analizar y anticipar de dónde vienen las probables amenazas y cuándo, aumentando su preparación
- Asegurar que todos en la organización comprendan la necesidad de una sólida gobernanza, controles de usuarios y rendición de cuentas.

Las organizaciones pueden no ser capaces de controlar cuándo ocurren incidentes de seguridad de la información, pero pueden controlar cómo responder a ellos, expandir las capacidades de detección es un buen punto de partida. Un buen funcionamiento del centro de operaciones de seguridad (*SOC*) puede formar el corazón de la detección efectiva.

90%

Perú

no tienen un programa de inteligencia de amenazas.

13%

Perú

tiene un plan de respuestas ante incidentes cibernéticos; sin embargo, no realizan mayor investigación sobre las causas principales.

La gestión de las amenazas cibernéticas de acuerdo con las prioridades del negocio debe ser el enfoque del *SOC*. Al correlacionar la información relevante para el negocio con una línea de base segura, el *SOC* puede producir informes relevantes, lo que permite una mejor toma de decisiones, gestión de riesgos y continuidad del negocio. Un *SOC* puede habilitar las funciones de seguridad de la información para responder con mayor rapidez, trabajar más en colaboración y compartir conocimientos de manera más eficaz.

Siga las prácticas más destacadas de seguridad cibernética

Al aprovechar las principales prácticas de la industria y adoptar estrategias que son flexibles y escalables, las organizaciones estarán mejor equipadas para hacer frente a los desafíos (a veces imprevistos) de su infraestructura de seguridad.

A medida que avanza la tecnología y las empresas continúan innovando a lo largo de los próximos años, las organizaciones que utilizan el *IoT* tendrán que evaluar continuamente las implicaciones de seguridad de adoptar estos avances. Una metodología consistente y ágil de evaluación de riesgos de seguridad en múltiples perspectivas ayudará a evaluar la exposición al riesgo de las organizaciones. La introducción de procedimientos apropiados y pruebas regulares ayudará a las organizaciones a ser más inteligentes y hará que sus empleados sean más conscientes de los desafíos que el *IoT* plantea para toda la empresa.

- **Conozca su entorno, por dentro y por fuera**
  El conocimiento integral, pero orientado, de la situación es crítico para entender el panorama más amplio de la amenaza y cómo se relaciona con la organización. La inteligencia de la amenaza cibernética puede aportar este conocimiento - incorpora fuentes de riesgo tanto externas como internas y cubre tanto el presente como el futuro, mientras se aprende del pasado.
- **Aprenda y desarrolle continuamente**
  Nada es estático - ni los criminales, ni la organización ni ninguna parte de su entorno operativo - por lo tanto, el ciclo de mejora continua se mantiene. Conviértase en una organización de aprendizaje: estudie los datos (incluidos los forenses), mantenga y explore nuevas relaciones colaborativas, actualice la estrategia regularmente y desarrolle las capacidades de seguridad cibernética.

- **Tenga confianza en su respuesta ante incidentes y mecanismos de respuesta ante crisis**
  Las organizaciones que están en un estado de anticipación ensayan regularmente sus capacidades de respuesta ante incidentes. Esto incluye juegos de guerra y ejercicios de mesa, hasta la realización de escenarios de incidentes complejos que realmente ponen a prueba las capacidades de la organización.
- **Alinee la seguridad cibernética con los objetivos empresariales**
  La seguridad cibernética debería convertirse en un asunto permanente de los comités de gerencia, un tema de vital importancia en la agenda. El liderazgo de la organización debe comprender y discutir cómo la seguridad cibernética permite al negocio innovar, abrir nuevos canales para comercializar y gestionar el riesgo. Para tener éxito, la función de seguridad de la información necesita apoyo del liderazgo para proporcionar los ingresos adecuados para apoyar y mejorar la protección de la seguridad, promover la conciencia cibernética dentro de la fuerza de trabajo y patrocinar la cooperación con compañeros de negocios.

Pase de la seguridad como un costo a la seguridad como una inversión

La seguridad se suele colocar como un costo obligatorio - un costo a pagar para cumplir o un costo a pagar para reducir el riesgo. Pero pasar a un modelo de seguridad como gestión de riesgo y confianza implica considerar la seguridad como un facilitador de negocios. Por ejemplo, la gestión del acceso a datos del consumidor aprovecha el valor monetario de los datos en lugar de centrarse en la protección de los datos en sí. De hecho, esta transformación permite el desarrollo de redes aún más amplias, de mayor cantidad y nuevas formas de colaboración y movilidad y de nuevos modelos de negocio. **"La seguridad como una inversión" debe ser un pilar del negocio**.

El futuro del *IoT*

Apodado por muchos como nada menos que la tercera revolución industrial, el Internet de las Cosas es uno de los elementos de cambio en el ámbito digital. Creemos que cuando todos y todo está interconectado dentro de redes de información sin fisuras y los datos resultantes se evalúan mediante grandes análisis de datos inteligentes y predictivos, y con medidas robustas de seguridad cibernética, veremos cambios positivos en la forma en que todos llevamos a cabo negocios; cómo operamos nuestras fábricas, cadenas de suministro y redes logísticas; cómo manejamos nuestra infraestructura; y por último pero no menos importante, cómo nosotros como consumidores, pacientes y ciudadanos interactuamos con proveedores, minoristas, proveedores de atención médica y agencias gubernamentales.

Paul van Kessel,
Líder de Seguridad Cibernética - EY Global

¿Cómo puede ayudar EY?

EY ha identificado que las respuestas de las organizaciones al crimen cibernético recaen en tres diferentes etapas de la madurez en seguridad cibernética – Activar, Adaptar y Anticipar (las tres As) – y el enfoque debería estar en implementar medidas de seguridad cibernética cada vez más avanzadas en cada etapa.

Etapa 1: Activar

Las organizaciones necesitan tener una base sólida de seguridad cibernética. Esto incluye un conjunto completo de medidas de seguridad de la información que proporcionarán una defensa básica (pero no buena) contra los ataques cibernéticos. En esta etapa, las organizaciones establecen sus principios, por ejemplo: ellos activan su seguridad cibernética

Etapa 2: Adaptar

Las organizaciones cambian ya sea para sobrevivir o para crecer. Las amenazas también cambian. Por lo tanto, el fundamento de las medidas de seguridad de la información debe adaptarse para mantener el ritmo y adaptarse a los cambios de las necesidades del negocio y su dinámica, de lo contrario será cada vez menos eficaz en el tiempo. En esta etapa, las organizaciones trabajan para mantener su seguridad cibernética al día; es decir, se adaptan a las necesidades cambiantes.

Etapa 3: Anticipar

Las organizaciones necesitan desarrollar tácticas para detectar y disminuir posibles ataques cibernéticos. Deben saber exactamente lo que necesitan para proteger sus activos más valiosos y ensayar las respuestas apropiadas a posibles escenarios de ataque o incidente: esto requiere una capacidad madura de inteligencia sobre amenazas cibernéticas, una sólida metodología de evaluación de riesgos, un mecanismo experimentado de respuesta ante incidentes y una organización informada. En esta etapa, las organizaciones confían más en su capacidad para manejar más amenazas previsibles y ataques inesperados; es decir, anticipan ataques cibernéticos.

¿Qué es?	Bloques de construcción del sistema de seguridad cibernética	Estado
Anticiparse es mirar hacia lo desconocido. Con base en la inteligencia de amenazas cibernéticas, se identifican brechas potenciales; las medidas se toman antes de que se produzca cualquier daño.	**Anticipar**	**Anticipar** es un nivel emergente. Cada vez más organizaciones están utilizando la inteligencia sobre amenazas cibernéticas para adelantarse al delito cibernético. Es una adición innovadora a la de abajo.
Adaptarse se trata del cambio. El sistema de seguridad cibernética está cambiando cuando el entorno está cambiando. Se centra en la protección del negocio del mañana.	**Adaptar**	El **Adaptarse** todavía no se ha implementado ampliamente. No es una práctica común evaluar las implicancias de seguridad cibernética cada vez que una organización realiza cambios en el negocio.
Activar establece el escenario. Se trata de un conjunto complejo de medidas de seguridad cibernética enfocadas a proteger el negocio de hoy.	**Activar**	**Activar** es parte del sistema de seguridad cibernética de toda organización. Todavía no se han tomado todas las medidas necesarias; todavía hay mucho por hacer.

Ayudándote a anticipar el crimen cibernético

Hemos visto que las organizaciones necesitan cambiar su forma de pensar para dejar de ser simplemente reactivas ante futuras amenazas; sin embargo, en nuestra reciente **Encuesta Global de Seguridad de la Información** descubrimos que sólo **el 64%** de las 1.735 organizaciones encuestadas no tienen o sólo tienen un sistema informal de inteligencia contra amenazas.

La única manera de adelantarnos a los criminales cibernéticos es aprender a anticipar sus ataques. Esto significa que su capacidad de seguridad cibernética debe ser capaz de abordar las siguientes preguntas:

- ¿Qué está pasando afuera que nuestra compañía tiene que aprender?
- ¿Cómo están lidiando con amenazas y ataques otras organizaciones exitosas?
- ¿Cómo puede nuestra organización volverse empedernida frente al ataque?
- ¿Puede nuestra organización distinguir entre un ataque al azar y uno dirigido?
- ¿Cuál sería el costo económico de un ataque?
- ¿Cómo se verían impactados nuestros consumidores por un ataque?
- ¿Cuáles serían las consecuencias legales y regulatorias de un ataque serio?
- ¿Cómo podemos ayudar a otros en nuestro ecosistema a lidiar con amenazas y ataques?

EY puede ayudar a las organizaciones a mejorar su capacidad para responder a los cambios en un panorama de amenazas. Ofrecemos servicios para ayudar a las organizaciones a desarrollar programas internos de inteligencia sobre amenazas, así como servicios clave de inteligencia sobre amenazas con modelos basados en suscripción y un espectro completo de servicios de inteligencia sobre amenazas cibernéticas.

En el 2016, el **56%** de las organizaciones no tenían un rol o departamento de seguridad de la información que se enfoque en identificar y gestionar vulnerabilidades, además de instalar Defensa Activa.

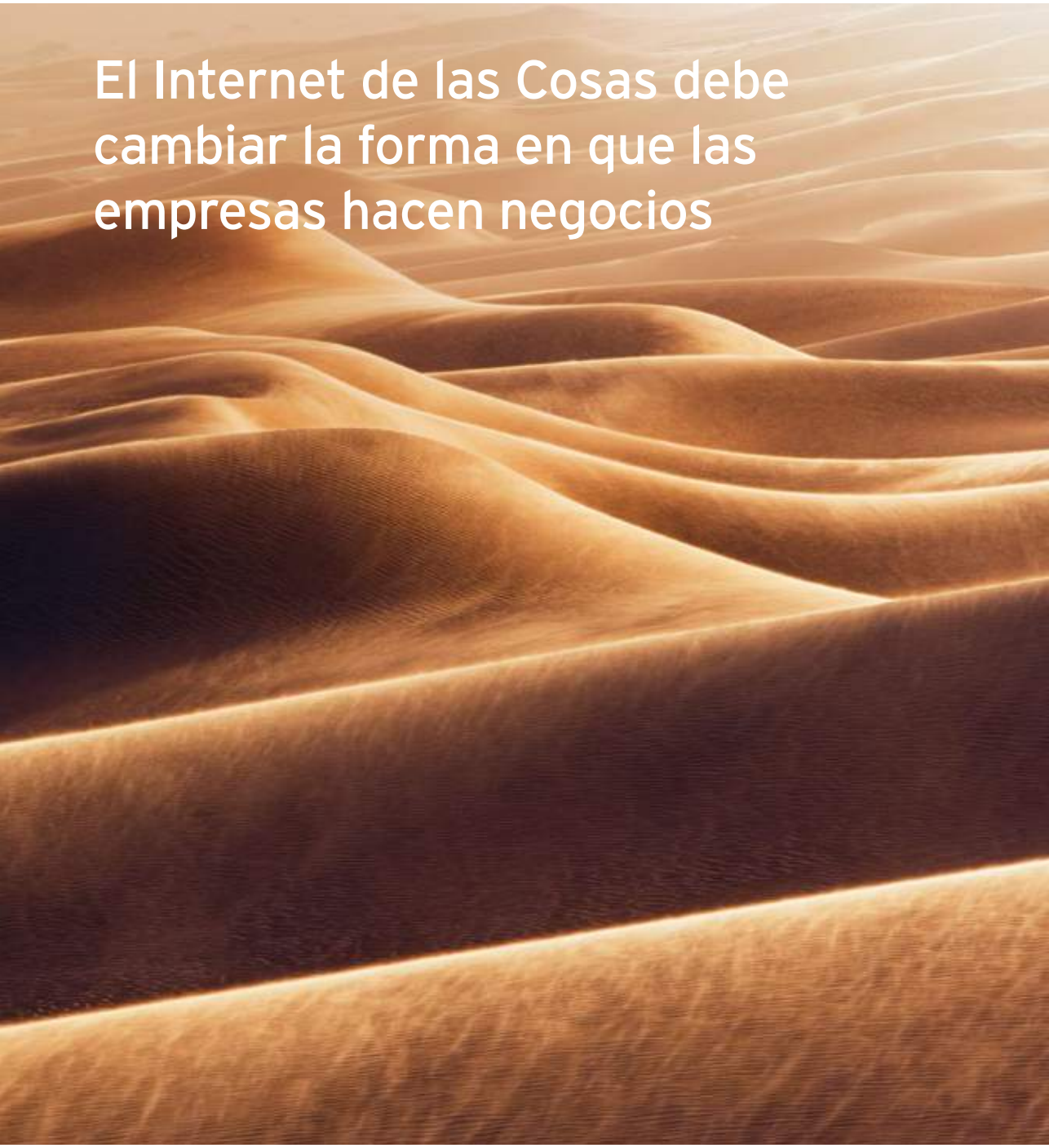
Creemos que las evaluaciones de seguridad son un método efectivo para identificar las vulnerabilidades y comprender su impacto. Junto con los grupos de seguridad de TI, gestión de riesgos y auditoría interna de nuestros clientes, contextualizamos estos hallazgos técnicos dentro de la empresa para comprender el riesgo de los activos más críticos. Es esta combinación de pruebas técnicas y dueños de negocios que creemos que seguirá siendo el método más efectivo para evaluar la seguridad de las tecnologías tanto definidas como emergentes.

Utilizando las prácticas de seguridad de EY y la experiencia líder de la industria, ayudamos a nuestros clientes a proteger tanto su ecosistema de dispositivos como a evaluar la seguridad a nivel de red, y ayudamos a nuestros clientes a definir e implementar controles de seguridad de última generación para:

- Asegurar los datos del dispositivo al centro de datos y a la nube
- Administrar grandes volúmenes de datos, utilizando conocimientos de análisis de datos
- Cumplir con los requisitos de seguridad y normas aplicables
- Estandarizar los controles de seguridad para sus ofertas, creando así capacidades de *go-to-market* más rápidas

Sin embargo, entendemos que muchos de nuestros clientes enfrentan restricciones de ubicación, tiempo y costo, lo que dificulta determinar qué medidas de seguridad son rentables y tienen sentido dentro de la estrategia empresarial. Nosotros podemos ayudar a nuestros clientes a obtener una comprensión completa de las opciones.

Conclusión



El Internet de las Cosas debe cambiar la forma en que las empresas hacen negocios

No hay duda de que el *IoT* está cambiando la forma en que todos vivimos y trabajamos. Existen muchas oportunidades tanto para el público como para los mercados del sector privado a través de la integración y colaboración tecnológica.

Se están introduciendo nuevas innovaciones diariamente, pero junto con éstas, se están creando amenazas que desafiarán a su organización. Usted necesita estar un paso adelante en el juego ahora para tener éxito mañana.

El *IoT* tendrá cada vez más herramientas de detección, análisis y visualización a las que se podrá acceder a nivel personal, comunitario o nacional. El intercambio de información y la facilidad de acceso a través del *IoT* hacen que las empresas sean vulnerables a ataques cibernéticos específicos, por lo que los enormes beneficios deben sopesarse frente a los crecientes riesgos.

> El *IoT* ofrece enormes oportunidades para mejoras personales y para la innovación de negocios, pero los innovadores deben ser conscientes de los riesgos involucrados en el *IoT* para proporcionar mejores y más poderosas soluciones para el mundo.

Como consecuencia de la adopción del *IoT*, junto con tecnologías y servicios de apoyo basados en infraestructura en la nube y dispositivos móviles, los requisitos de seguridad de la empresa deben abordarse con un enfoque en las relaciones entre la organización y su entorno.

Las organizaciones deben adaptarse y mirar hacia adelante y más allá del negocio actual. Con la comprensión de que los ataques nunca pueden ser completamente evitados, las compañías deben avanzar en sus capacidades de detección de amenazas cibernéticas para que puedan responder de manera adecuada y proactiva.

Aprender a mantenerse a la vanguardia de la delincuencia cibernética es desafiante y lleva tiempo, pero los beneficios para la organización son considerables: la organización podrá aprovechar las oportunidades que ofrece el mundo digital, minimizando la exposición a los riesgos y el costo de lidiar con ellos.

Siguientes pasos

Eche un vistazo a su organización, ¿qué puede hacer que no podía hacer antes? Empiece a hacerlo ahora, antes que alguien más lo haga. Tome acción en lugar de reaccionar.

Considere las siguientes preguntas clave:

- ¿Qué capacidades del *IoT* tiene su organización hoy en día?
- ¿Puede aprovechar las ideas complementarias tanto del servicio como de los líderes de TI?
- ¿Ha identificado áreas importantes de oportunidad del *IoT* que se relacionan con su visión y estrategia?
- ¿Se puede construir una cultura del *IoT* en torno a las posibilidades de conectar lo no conectados?
- ¿Cómo cambiará el *IoT* la base de la competencia?
- ¿Cómo deleitará a sus clientes cuando todo se conecte?
- ¿Sus planes de negocio reflejan todo el potencial del *IoT*?
- ¿Están sus inversiones tecnológicas alineadas con oportunidades y amenazas?
- ¿Cómo el *IoT* mejorará su agilidad?
- ¿Tiene las capacidades para ofrecer valor del *IoT*?
- ¿Cuál es su estructura/modelo de rendición de cuentas y gobernabilidad para la ejecución del *IoT*?
- ¿Cómo están siendo abordados los riesgos asociados con el *IoT*?
- ¿Cómo les comunicará acerca del *IoT* a las partes interesadas?

Contactos
EY Perú

Paulo Pantigoso
Country Managing Partner
paulo.pantigoso@pe.ey.com

Consultoría

Jorge Acosta
Socio Líder de Consultoría
jorge.acosta@pe.ey.com

Elder Cama
elder.cama@pe.ey.com

Giuliana Guerrero
giuliana.guerrero@pe.ey.com

Fabiola Juscamaita
fabiola.juscamaita@pe.ey.com

Víctor Menghi
victor.menghi@pe.ey.com

Geraldine Mouchard
geraldine.mouchard@pe.ey.com

Cecilia Ota
cecilia.ota@pe.ey.com

Renato Urdaneta
renato.urdaneta@pe.ey.com

Raúl Vásquez
raul.vasquez@pe.ey.com

Consultoría para la Industria Financiera

José Carlos Bellina
Socio Líder de Consultoría para la Industria Financiera
jose.bellina@pe.ey.com

Numa Arellano
numa.arellano@pe.ey.com

Alejandro Magdits
alejandro.magdits@pe.ey.com

Oficinas

Lima
Av. Víctor Andrés Belaúnde 171,
San Isidro – Lima
Telf: +51 1 411 4444

Arequipa
Av. Bolognesi 407,
Yanahuara – Arequipa
Telf: +51 54 484 470

Chiclayo
Av. Federico Villarreal 115, Salón Cinto,
Chiclayo – Lambayeque
Telf: +51 74 227 424

Trujillo
Av. El Golf 591, Urb. Del Golf III Etapa.
Víctor Larco Herrera 13009,
Sala Puémape, Trujillo – La Libertad
Telf: +51 44 608 830

Si usted estuviera bajo un ataque cibernético, ¿lo sabría?

Para EY, un mundo que funciona mejor significa resolver grandes problemas en industrias complejas y aprovechar las oportunidades para entregar resultados que hagan crecer, optimizar y proteger los negocios de nuestros clientes. Contamos con un equipo de consultores, profesionales de la industria y socios con un enfoque en mente. Consideramos que anticiparse, y ahora defenderse, activamente contra los ataques cibernéticos es la única forma de llevar la delantera a los delincuentes cibernéticos. Con nuestro enfoque centrado en usted, hacemos mejores preguntas sobre sus operaciones, prioridades y vulnerabilidades. Luego trabajamos con usted para crear respuestas más innovadoras que ayuden a ofrecer las soluciones que usted necesita. Juntos lo ayudaremos a obtener mejores resultados y más duraderos, desde la estrategia hasta la ejecución.

Creemos que cuando las organizaciones manejen mejor la seguridad cibernética, el mundo funcionará mejor. Entonces, si usted estuviera bajo un ataque cibernético, ¿lo sabría? Pregúntele a EY.

Mientras mejor es la pregunta, mejor es la respuesta, y mejor funciona el mundo.

EY | Advisory | Assurance | Transactions | Tax

Acerca de EY
EY es el líder global en servicios de auditoría, impuestos, transacciones y consultoría. La calidad de servicio y conocimientos que aportamos ayudan a brindar confianza en los mercados de capitales y en las economías del mundo. Desarrollamos líderes excepcionales que trabajan en equipo para cumplir nuestro compromiso con nuestros stakeholders. Así, jugamos un rol fundamental en la construcción de un mundo mejor para nuestra gente, nuestros clientes y nuestras comunidades.

Para más información visite **www.ey.com**

EY PERU LIBRARY

Descargar nuestras publicaciones y guías en:
ey.com/PE/EYPeruLibrary

/EYPeru

@EYPeru

/company/ernstandyoung

YouTube EYPeru

perspectivasperu.ey.com

ey.com/pe