Servicios de Consultoría

Generando confianza en el mundo digital

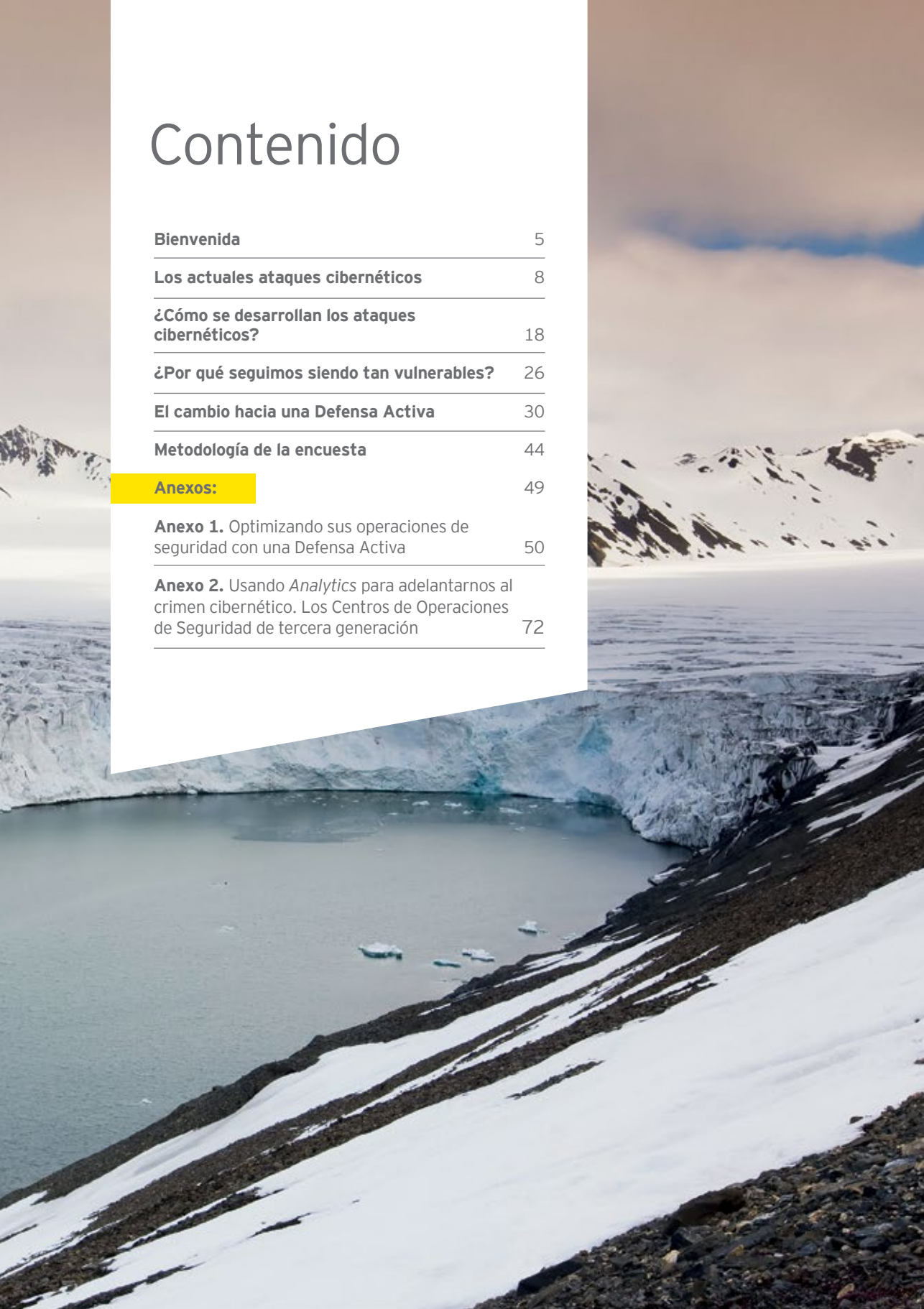
Perspectivas sobre Gobierno, Riesgo y Cumplimiento

Encuesta Seguridad de la información 2015

| ABRIL 2016

EY
Building a better working world

Contenido



Bienvenida

Tengo el agrado de presentar el informe de resultados de nuestra 18 ava **Encuesta Global de Seguridad de la Información 2015, "Generando confianza en el mundo digital"**, el cual analiza los más importantes incidentes y tendencias de seguridad cibernética que enfrentan hoy en día las compañías.

Este año nos ha complacido contar con 1,755 participantes a nivel mundial; entre ellos, representantes de empresas peruanas, a los cuales les queremos agradecer por el tiempo dedicado a contestar la encuesta.

En el 2014, identificamos medidas que las empresas podían implementar para enfrentar el crimen cibernético. Estas medidas aún son aplicables; sin embargo, como los ataques cibernéticos son cada vez más complejos, la naturaleza de las amenazas cibernéticas también ha ido evolucionando.

Si aún está tratando de entender cómo manejar esta situación, no está solo. Más de un tercio de los participantes en nuestra encuesta considera que es poco probable que puedan identificar un ataque sofisticado, y en nuestra experiencia, solo las compañías que están más alertas podrán identificar aquellas pequeñas anomalías que son el inicio de una brecha mayor.

La seguridad cibernética posee un alcance que contempla temas más allá de la tecnología, por lo cual no puede mantenerse solamente en el dominio de las áreas de Tecnología y Sistemas de Información. Tampoco puede ser responsabilidad de un miembro del Directorio, ya que afecta a los diferentes niveles de la compañía, con diferentes niveles de complejidad.

Este documento muestra cómo las organizaciones deben trabajar de manera coordinada a fin de consolidar los recursos necesarios para un mejor análisis de riesgos. Nuestra experiencia en seguridad cibernética nos demuestra que debemos mantenernos en un estado constante de "Defensa Activa". Así mismo, hemos incorporado una sección acerca de la importancia del uso de Analytics para la prevención de crímenes cibernéticos.

Reiteramos nuestro agradecimiento a nuestros clientes por su participación en la encuesta y esperamos que el presente documento ayude a generar conciencia y conocimiento sobre un tema tan relevante y de actualidad como la seguridad cibernética.

Atentamente,

Jorge Acosta
Socio Líder
Advisory Services

Comprendiendo los desafíos de la seguridad cibernética

El mundo digital está lleno de oportunidades de rápida expansión para la innovación. Los gobiernos y organizaciones han dirigido su atención hacia los beneficios significativos que esto implica, creando nuevos mercados y productos para lograr un mejor conocimiento de los consumidores, y encontrar diferentes y mejores formas de conectarnos con ellos.

Desafortunadamente, debido a su rápido crecimiento, muchos controles de seguridad han sido pasados por alto y algunos riesgos han sido subestimados. La comprensión de la existencia de amenazas de seguridad y del potencial que tiene el mundo digital de ser explotado por criminales, ha llegado demasiado tarde.

Para que las organizaciones reconozcan los desafíos actuales y entiendan lo que es necesario hacer, deben analizar cada una de las siguientes cuatro áreas:

Los actuales ataques cibernéticos

- ¿Cómo está cambiando el mundo y cómo afecta a nuestra organización?
- ¿Cuáles son las amenazas y vulnerabilidades que debemos tener en cuenta?
- ¿Cómo podemos enfrentar los ataques cibernéticos?

¿Cómo se desarrollan los ataques cibernéticos?

- ¿Cuáles son los peores escenarios que se podrían presentar?
- ¿Cómo podemos detectarlos de manera oportuna?
- ¿Por qué debemos estar en alerta máxima?

¿Por qué seguimos siendo tan vulnerables?

- No se toman las medidas suficientes en nuestras organizaciones.
- No contamos con ningún mecanismo que nos permita adaptarnos a los cambios.
- No poseemos mecanismos que permitan controlar los ataques de manera oportuna.

El cambio hacia una Defensa Activa

- ¿Qué es la Defensa Activa?
- ¿Que debemos mejorar?
- ¿Cómo implemento la Defensa Activa?

Los actuales ataques cibernéticos

¿Cómo está cambiando el mundo y cómo afecta nuestra organización?

Las organizaciones no tienen más alternativa que seguir operando en este entorno digital en constante evolución, de modo que inevitablemente existe un creciente interés en conocer las actuales amenazas e incidentes cibernéticos y cómo éstos podrían afectarnos. Es inaceptable que roben información y data personal de clientes, y es claro que el robo de la propiedad intelectual, así como las pérdidas y los costos posteriores incurridos para remediarlos generan perjuicios en nuestra organización. Los *hackers*, la manipulación de los medios de comunicación y de los sistemas de administración y defensa de los gobiernos, son reconocidos como una amenaza significativa para la seguridad nacional.

Entonces, ¿Qué significa sobrevivir en el mundo digital?

Para analizar a su organización a nivel cibernético se deben considerar las siguientes áreas:

Utilizando la seguridad cibernética para lograr la sostenibilidad digital
Dimensiones de la compañía

Global

88%

Perú

100%

de los encuestados considera que su seguridad de la información no cubre plenamente las necesidades de su organización.

Global

68%

Perú

91%

de los encuestados no considera monitorear el ecosistema de su negocio como un esquema de seguridad de la información en Internet.

Operar en un mundo digital – ¿Qué es lo que ha cambiado?

- Los dispositivos "*smart*" y servicios inteligentes nos permiten acceder y consolidar nuestra información; en consecuencia, han incrementado la cantidad de vulnerabilidades y mecanismos para su explotación.
- Las redes sociales y BYOD (Traiga su Propio Dispositivo), mantienen a empleados, clientes y ciudadanos "siempre conectados" y compartiendo información, sin evaluar las consecuencias que puedan tener sobre la privacidad y confidencialidad de su información.
- Las organizaciones alojan cada vez más datos en la nube (*"Cloud")* y en instalaciones de terceros; lo cual es atractivo, pero peligroso, debido a la pérdida de control y existencia de nuevas amenazas, en un ecosistema complejo.
- El comportamiento de las personas evoluciona de manera impredecible.
- Existen nuevas legislaciones y regulaciones que están forzando un cambio en los procesos. A su vez, se crean nuevas vulnerabilidades, que cambian aún más los escenarios, el entorno de las amenazas (a menudo ampliándolo, no reduciéndolo) y las áreas de ataque, en una organización.

¿Cuáles son las amenazas y vulnerabilidades que debemos tener en cuenta?

Para que su organización sea un lugar más seguro y más sostenible en el mundo digital, es necesario aplicar un análisis de riesgos de seguridad cibernética a todo nivel.

Muchas organizaciones están tomando un enfoque "clásico" para manejar sus riesgos y vulnerabilidades, exponiéndolos a amenazas más grandes. Ésta no es una responsabilidad que pueda ser delegada a una o dos personas; estas responsabilidades se deben definir en un amplio rango de personas en toda la organización, y deben reunirse para formar una sola visión coherente y coordinada. Esta visión, por un lado, tendrá una presentación distinta para el Directorio y la alta gerencia, y otra para los empleados. Asimismo, se presentará diferente para los socios, proveedores, vendedores y terceros.

El problema es cómo lograr evitar ahogarse entre toda esta información sin crear más trabajo ni riesgos innecesarios. Al contrario, se debe priorizar, agilizar y mapear lo que significa para su organización un enfoque completo e integral de seguridad cibernética. Los componentes básicos podrán ser comunes; sin embargo, sólo se obtendrá un valor completo concibiendo el enfoque de seguridad cibernética desde su estrategia de negocio, sus riesgos y prioridades.

Para guiar a su organización de manera eficiente a través de los niveles de riesgos y amenazas, los líderes deben tener confianza al momento de fijar el apetito de riesgo y estar preparados para tomar una acción decisiva a fin de gestionar cualquier incidente. Por ejemplo, un tema claro que surge desde los dos últimos años es que el impacto de un incidente es reducido mayormente por un análisis inteligente y apropiado de incidentes cibernéticos, y una comunicación efectiva, tanto externa como interna.

¿Qué preguntas debemos analizar en nuestra organización?

- ¿Estamos seguros que comprendemos las amenazas y vulnerabilidades en el mundo digital?
- ¿Hemos analizado qué necesitamos para poder identificar las amenazas que podrían impactar a nuestra organización, su estrategia, y qué medidas de seguridad cibernética debemos aplicar para controlarlas?
- ¿Sabemos cómo determinar el apetito de riesgo, así como la pérdida y los daños aceptables e inaceptables que resulten de posibles incidentes de seguridad por amenazas cibernéticas?

Sólo cuando el apetito de riesgo esté fijado a un nivel con el cual el Directorio se sienta cómodo, y que la organización lo pueda alcanzar, entonces los cambios digitales serán sostenibles.

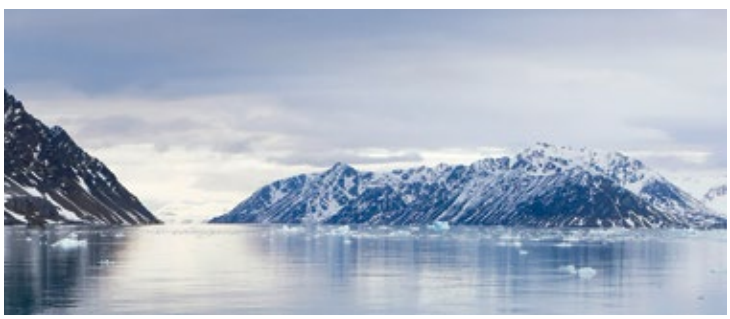
Global

67%

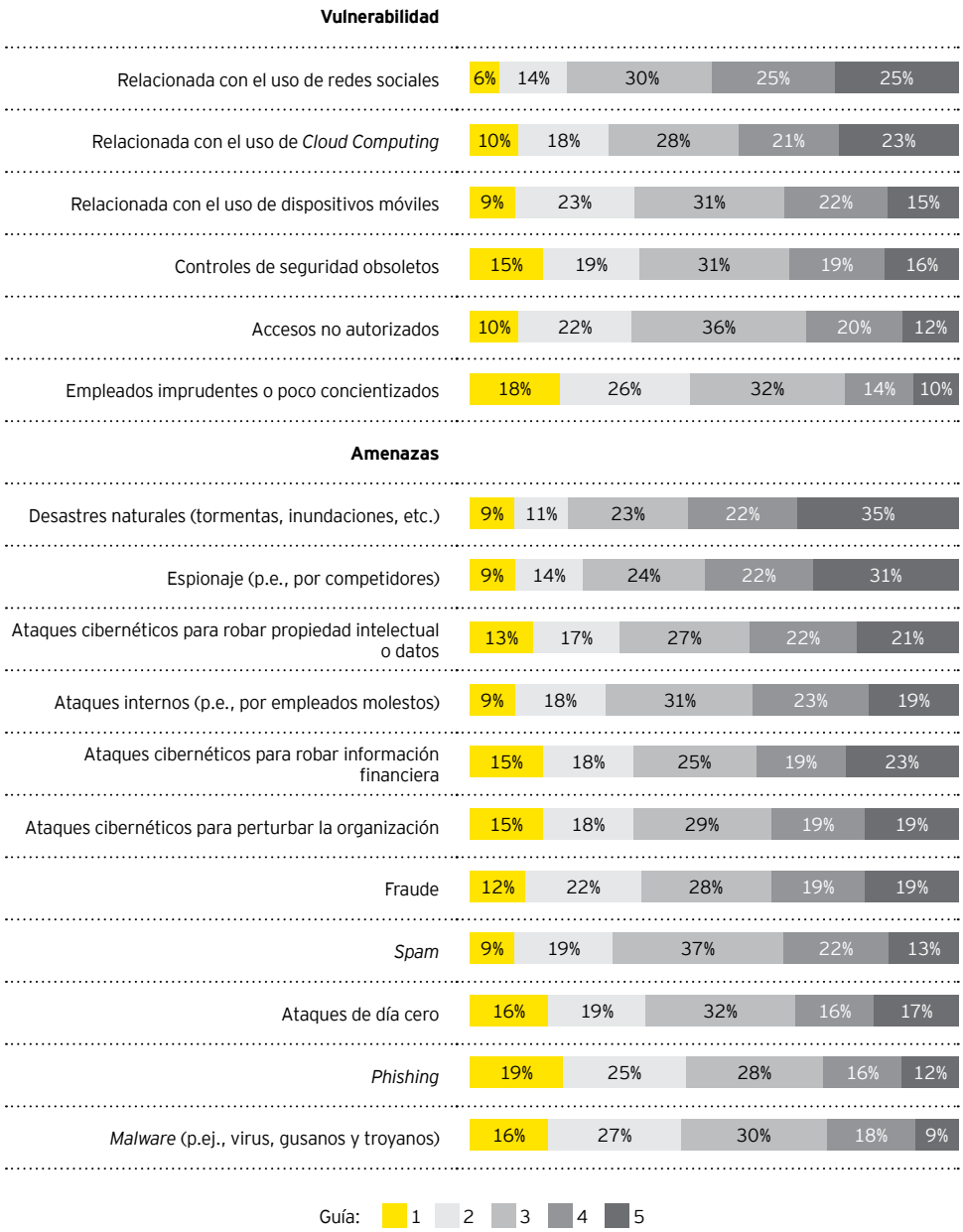
Perú

97%

de los encuestados no ve a la gestión de los accesos como un creciente desafío de seguridad cibernética.



¿Qué amenazas* y vulnerabilidades han incrementado más su exposición al riesgo en los últimos 12 meses?** (Considerar todos estos ítems, con 1 como prioridad más alta, y 5 como su prioridad más baja)



* Amenaza se define como la posibilidad de una acción adversa por parte de factores externos
** Vulnerabilidad se define como la exposición existente a la posibilidad de ser atacado o dañado

¿Cómo se comparan los resultados del 2015 con los del 2014?

Si observamos las dos vulnerabilidades más altas:

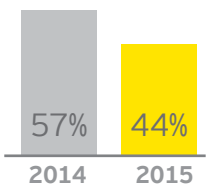
- Empleados imprudentes o poco concientizados
- Controles de seguridad obsoletos

En 2014, estas dos vulnerabilidades eran percibidas como prioridades alta y más alta, pero el grado de vulnerabilidad que sienten las organizaciones ha disminuido en estas áreas. Hoy, solo el 44% se siente vulnerable con respecto a empleados imprudentes, en comparación con el 57% en 2014; solo el 34% se sienten vulnerables debido a sistemas obsoletos, en comparación con el 52% en 2014. Esto muestra que las organizaciones creen que están cubriendo sus vulnerabilidades de manera más eficaz.

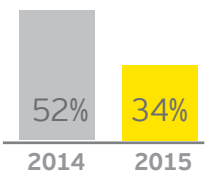
Sin embargo, cuando observamos las dos amenazas más altas de hoy:

- *Phishing*
- *Malware*

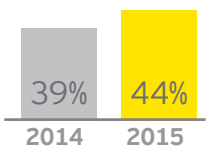
Estas amenazas figuraron en el 5to y 7mo lugar en el año 2014, junto al robo de información financiera, propiedad intelectual, la amenaza de fraude, espionaje y ataques de día cero, todos considerados como más altos. Esta percepción tan exacerbada del *phishing* y el *malware* como amenazas demuestra un cambio claro de perspectiva, pero ¿es este el cambio correcto o sólo una tendencia a una dirección equivocada?



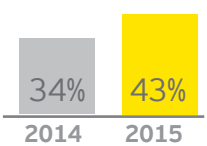
Hoy, solo el 44% de organizaciones se sienten vulnerables con respecto a empleados imprudentes en comparación con el 57% en el 2014.



Solo el 34% de organizaciones se sienten vulnerables debido a los sistemas obsoletos, en comparación con el 52% en el 2014.



Hoy en día, el 44% de organizaciones ve al *phishing* como la amenaza más alta en comparación con el 39% en el 2014.



Hoy en día, el 43% de organizaciones ve al *malware* como la amenaza más alta en comparación con el 34% en el 2014.

Global

42%

Perú

6%

de los encuestados dice que conocer todos sus activos es un desafío de seguridad de la información.

¿Cómo podemos enfrentar ataques cibernéticos?

Sin ninguna duda su organización enfrentará incidentes cibernéticos. Esto ya es parte integral del mundo digital.

El punto de partida para generar confianza en la organización es analizar continuamente la forma en que somos vistos ante un atacante cibernético.

- **¿Cómo puede proteger a su organización ante un incidente cibernético si usted no conoce los objetivos de los atacantes?**
- **¿Cómo podrían obtener acceso y afectar sus activos críticos de la organización?**
- **¿Cómo puede estar seguro si no conoce plenamente la capacidad de su organización para responder, contener y recuperarse de un ataque?**

Las organizaciones a menudo están familiarizadas con las mejores prácticas de gestión de riesgos y éste es un punto de partida útil para ponerse a pensar acerca de la seguridad cibernética.

Principios claves de la gestión de riesgos ...	... aplicados al riesgo cibernético
1 **Enfocarse en lo más importante** Alinearse a su cultura de negocio y riesgo.	**Conocer sus activos de información críticos** Identificar los activos de negocio críticos más vulnerables al ataque cibernético.
2 **Medir y reportar** Incluir evaluaciones cualitativos y cuantitativas.	**Hacer más tangible el riesgo cibernético** Definir claramente el riesgo cibernético y sus métricas fundamentales.
3 **De naturaleza integral** Cubrir todo tipo de riesgos, actuales y futuros.	**Alinearse con los marcos de riesgo existentes** Financiero, operativo, regulatorio, de cliente, de reputación, etc.
4 **Asignación del apetito al riesgo** Asignación del apetito al riesgo a unidades de negocio y tipos de riesgo.	**Hacer que el riesgo cibernético sea relevante para el negocio** Vincular los riesgos de nivel organizacional con las unidades de negocio individuales y sus activos de información.
5 **Integración con el planeamiento del negocio** Los reguladores están buscando cada vez más evidencias.	**Integrar el apetito de riesgo a las decisiones de inversión** Priorizar la inversión donde sea crítica, y empoderar a los gestores para que tomen decisiones de manera informada.

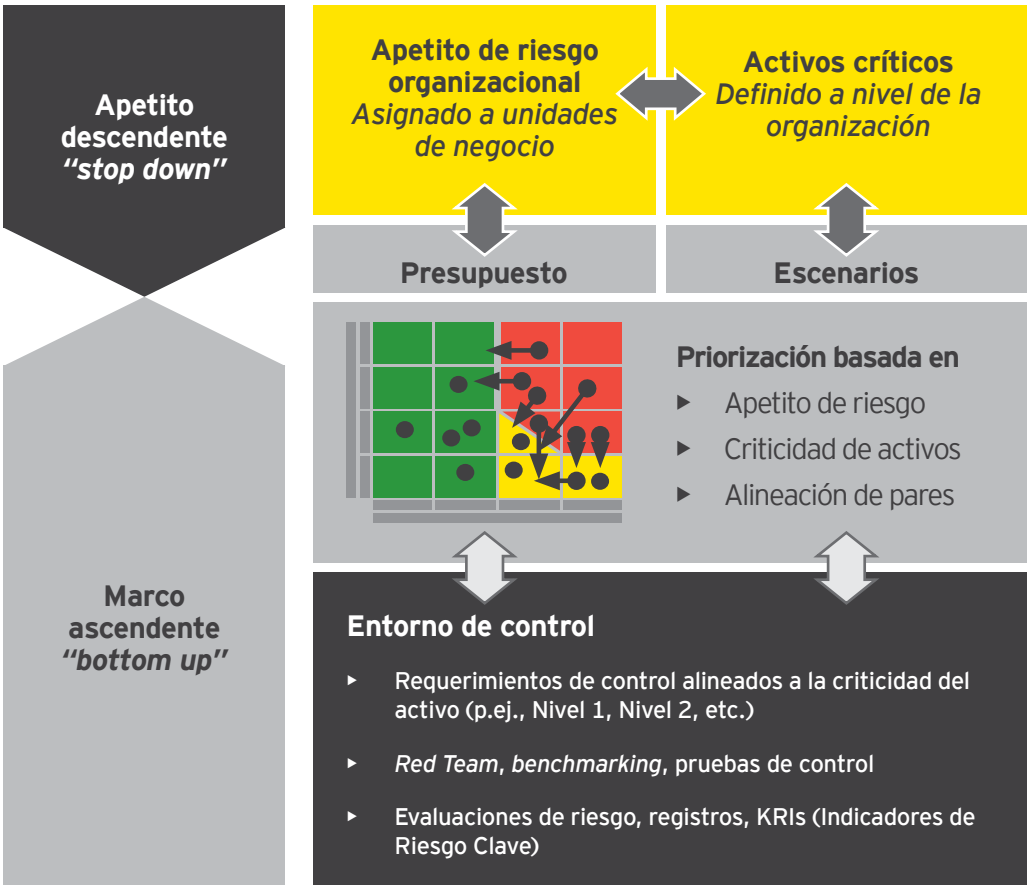
Global y Perú

20%

de los encuestados no puede estimar el daño financiero total relativo a los incidentes cibernéticos en los últimos 12 meses.

Los incidentes cibernéticos son a menudo anunciados como eventos drásticos y sensacionales con brechas masivas, sistemas y sitios inoperativos, resultando en inconvenientes o daños repentinos para los clientes. Los titulares se centran en los eventos de gran escala: robos de millones de datos, informaciones divulgadas en línea sin autorización, hurto de propiedad intelectual y sistemas dañados.

Sin embargo, la naturaleza repentina de estos titulares es engañosa. La mayoría de estos ataques empezaron semanas o meses antes, cuando los criminales cibernéticos encontraron su punto de entrada



Red Team: *Un Red Team es un grupo que desafía activamente a una organización para mejorar su seguridad a través de ejercicios específicos, tales como prueba de penetración, ingeniería social, etc.*

y empezaron pacientemente a explorar y a localizar activos valiosos para desarrollar sus planes de ataque.

Además, los incidentes cibernéticos no son eventos aislados, independientemente de cuán complejos o simples, aleatorios u orientados puedan ser, o parezcan ser. Las primeras señales y el impacto acumulativo de ataques repetitivos deben ser entendidos e incluidos en su planeamiento y en su definición de apetito de riesgo.

Identificar los riesgos actuales (*"top down"*)

- La definición *"top down"* del apetito de riesgo y los activos de información críticos.
- Mapear los activos críticos en todos los sistemas, el negocio, y en terceros.

Priorizar lo más importante

- Asumir que las infracciones ocurrirán – mejorar los controles y procesos para identificar, proteger, detectar, responder y recuperarse de los ataques.
- Equilibrar los fundamentos con las amenazas emergentes y las capacidades de los pares.

Dirigir y monitorear el desempeño

- Evaluar regularmente el desempeño y el riesgo residual.
- Medir los indicadores principales para identificar los problemas mientras aún son pequeños.

Optimizar las inversiones

- Aceptar los riesgos tolerables cuando no haya presupuesto disponible.
- Considerar siempre en toda inversión, el impacto en costos y la operativa del "día a día".

Establecer funciones del negocio

- Hacer que la seguridad sea la responsabilidad de todos.
- No restringir las tecnologías más recientes; usar las iniciativas de cambio para establecerlas.

¿Cómo se desarrollan los ataques cibernéticos?

¿Cuáles son los peores escenarios que se podrían presentar?

Para identificar una anomalía, primero se debe conocer el entorno como la palma de su mano y para ello, es necesario determinar cuáles podrían ser algunos de los escenarios de riesgo cibernético de mayor importancia, y analizar las situaciones de pérdida que causarían mayor daño a la organización. En base a ello, priorizar las medidas preventivas y establecer controles entorno a aquellas áreas más críticas y escenarios de posibles ataques.

Un ejemplo de escenario de ataque:

Una violación cibernética puede ser muy sutil – Varios incidentes que ocurren al mismo tiempo

Ingeniería social avanzada (ej., ataques de tipo *spear-phishing, watering hole*)

Recolección sofisticada de análisis de inteligencia en seis meses

Conocimiento total de las debilidades de la empresa — personas, procesos y tecnología

El efecto acumulativo en una organización puede ser grande

Ventas

La manipulación de los sistemas de ventas y correos electrónicos resulta en pérdida de **ventas de 2% a 3%** justo antes de los períodos de informes trimestrales o anuales.

Cadena de suministros

La manipulación de la cadena de suministro y del sistema de pedidos en línea conduce a la degradación de la producción y el cobro de cuentas por cobrar resultando en **proyecciones de pérdida de ingresos de 2% a 3%.**

Investigación y desarrollo

Robo en áreas de alta rentabilidad y esfuerzos de desarrollo de productos, resultando en la **pérdida de ventas y ventaja competitiva.**

Cuentas por pagar

El fraude sobre las cuentas por pagar causa **US$ millones en pérdidas por año.**
La liberación masiva de datos privados resulta en una pérdida de credibilidad pública y costos legales adicionales.

Impacto de devaluación

La organización es abordada por los posibles causantes del ataque cibernético para adquirir la entidad en problemas a un menor valor.

La devaluación artificial resulta en **Más de 30% de pérdida en el valor de la empresa**

Los rumores en las redes sociales resultan en **más de 50% de pérdida de en la capitalización de mercado (valor de mercado)**

Mercado

Valor del mercado bajado artificialmente para obtener ganancia financiera y facilitar la adquisición de una participación accionaria importante de empresas listadas a un menor valor.

Tiene impacto sobre las decisiones empresariales, fusiones/adquisiciones y sobre la posición competitiva

Con uno o más escenarios identificados en procesos importantes y riesgos cibernéticos, es posible definir qué áreas de la organización deben ser vigiladas más cuidadosamente que otras:

- ¿El robo de información podría afectar la reputación de mi organización?
- ¿Una caída del valor en el mercado podría impactar en mi preparación para mis futuras fusiones o adquisiciones importantes?
- ¿Contamos con una adecuada administración de la información que manejamos con terceros, en especial en las áreas de negocio más críticas?

¿Quién o qué considera usted que es la fuente de ataque más probable?

¿Los criminales cibernéticos están preparados?

Los criminales cibernéticos pueden pasar meses dentro de su organización, encontrando información que almacenarán para un futuro ataque o consolidando información que los llevará al premio que buscan, asimismo, crearán medidas para evitar ser detectados. Algunas veces crean tácticas de distracción para alejar su atención de lo que están haciendo y en dónde han tenido éxito. A menudo, los criminales conservan la información robada y no la usan por un tiempo – otras veces, la compartirán entre la comunidad de criminales cibernéticos (quizás por un precio), extendiendo aún más las amenazas directas contra usted.

Ocasionalmente, estas exploraciones criminales dejan rastros y se notarán algunas señales, pero no es muy fácil darse cuenta. Las señales son tan sutiles que no se comentan ni se reportan, por lo que no se relacionan a ningún escenario mayor. Aún si la seguridad cibernética fuera un ítem permanente en la agenda del Directorio, a menudo no será evidente que los pequeños eventos inexplicables que cada ejecutivo atiende por separado en su departamento, puedan ser parte de una violación cibernética más extensa y sofisticada con el potencial de provocar un daño mayor.

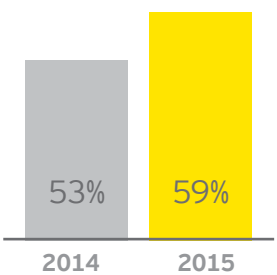
¿Cómo debemos detectarlo de manera oportuna?

Colocar la mayor atención, prevención y contramedidas alrededor de sus áreas de mayor valor y más alto riesgo es un paso clave para minimizar el daño que resulte de los incidentes cibernéticos. Ser capaz de detectar los incidentes cibernéticos de manera oportuna es el siguiente paso crucial, que sólo es posible con un radar integral que cubra una variedad de indicadores y que puedan emitir alertas cuando se cruce cierto umbral. La determinación de los umbrales se relaciona al apetito de riesgo y los tipos de incidentes que podrían causar el mayor daño a su organización.

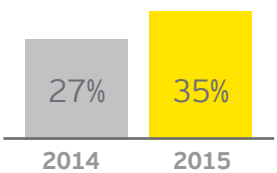
Algunos ataques son repentinos y obvios, en cuyo caso todo el enfoque se dirige hacia la respuesta inmediata. Sin embargo, recuerde que estos ataques obvios también pueden ser una táctica de distracción, así que las organizaciones necesitan tener la capacidad de analizar cada incidente con el fin de conseguir los datos suficientes para identificar patrones en el tiempo.

Existen muchas maneras para penetrar en una organización, y los atacantes cibernéticos encontrarán los puntos de entrada más vulnerables. Algunos de estos son obvios y, por lo tanto, más fáciles de controlar y monitorear, pero pensando creativamente en un escenario sobre cómo podrían operar los atacantes, pueden añadirse barreras y monitoreos adicionales a lugares no tan obvios (por ejemplo, sitios web de acceso público, sistemas de terceros que se conectan con los de usted, sistemas industriales de conexión, la nube, etc.).

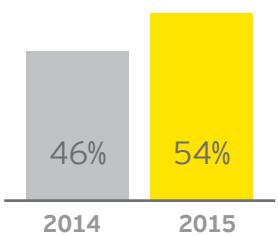
A nivel Global:



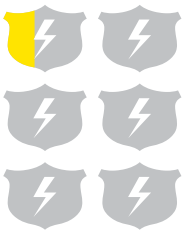
El 59% ve a los grupos criminales como la fuente más probable de ataque en la actualidad, en comparación con el 53% en el año 2014.



El 35% ve a los atacantes auspiciados por otros gobiernos como la fuente de ataque más probable en la actualidad, en comparación con el 27% en el año 2014.



El 54% ve a los *hacktivistas* como la fuente más probable de ataque en la actualidad, en comparación con el 46% en el 2014.



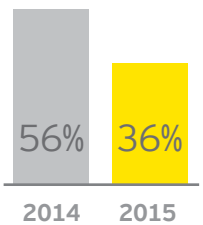
Global

7%

Perú

6%

de las organizaciones afirma tener un proceso robusto de respuesta ante incidentes que incluya a terceros y a las fuerzas del orden.



36% dice que es poco probable que fueran capaces de detectar un ataque sofisticado. Esto es una mejora significativa con respecto al 2014 en donde se observó un 56%. Pero las organizaciones deben recordar que el nivel de sofisticación aumenta permanentemente.

Una vez dentro, los atacantes se abrirán camino hasta los activos de "valor". Es aquí donde es esencial conocer sus prioridades de negocio, lo que más puede dañarle, y lo que tiene valor para sus clientes – el punto donde estos se intersectan es donde podrían ser detectables indicadores o señales más sutiles.

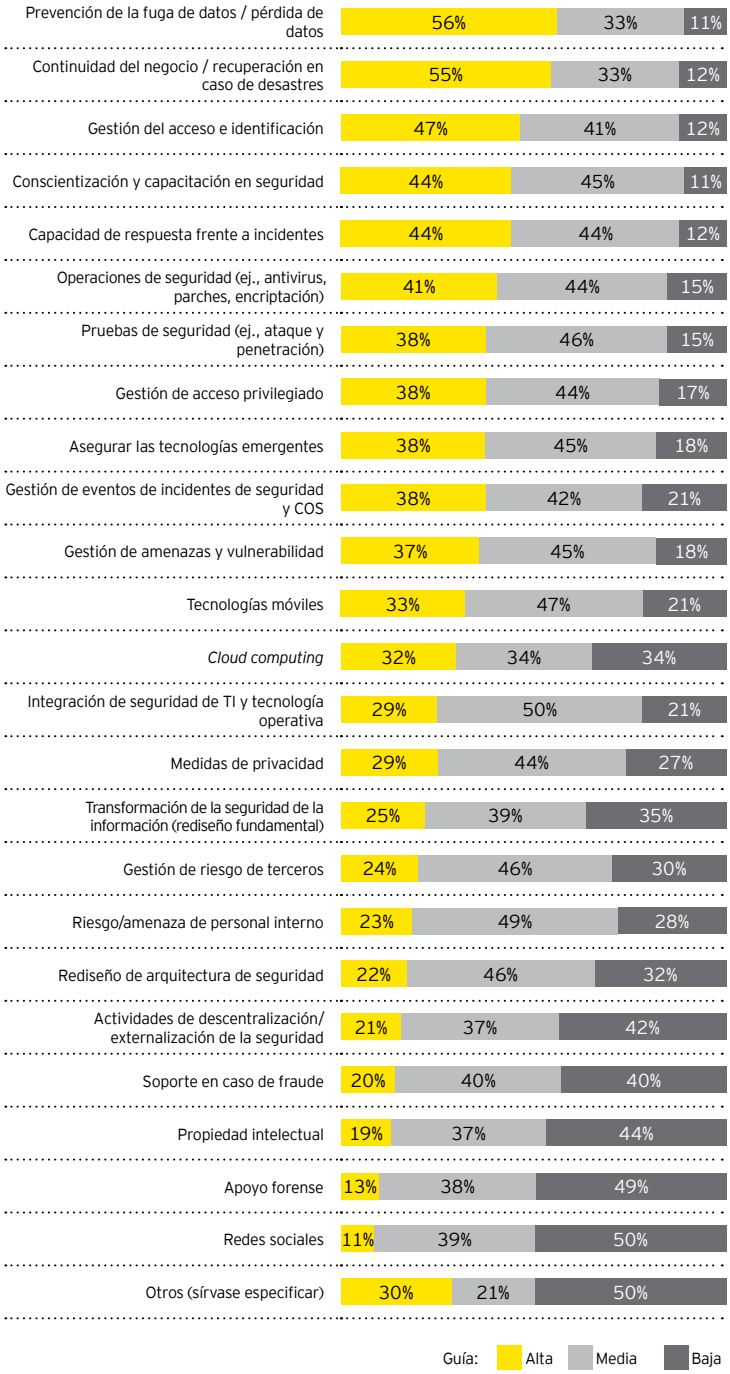
Los departamentos de Finanzas, Marketing, Operaciones, Investigación y Desarrollo y Recursos Humanos deben estar conscientes de los riesgos cibernéticos para la organización. Todos ellos necesitan estar en alerta para detectar comportamientos anómalos y estar listos para reportarlos al responsable de seguridad cibernética de tal manera que puedan añadirlos a sus otros reportes.

Al igual que con las campañas públicas contra el terrorismo, el mensaje es que no hará daño señalar algo que cause sospechas. El factor crítico es que se reporte a los responsables pertinentes, quienes pueden ensamblar el rompecabezas.

Ejemplos de indicadores que se deben monitorear:

- Ataques visibles sin una finalidad evidente: ej., hurto de datos sin una finalidad específica.
- Movimientos inesperados de precio de acciones.
- Nuevos productos lanzados por los competidores que son extrañamente similares a los de su organización y que alcanzan el mercado justo antes que los de usted – indicando un robo de propiedad intelectual y conocimiento de la estrategia de crecimiento.
- Fusiones y Adquisiciones (M&A) suspendidas: propuestas de competidores que muestran similitudes y podrían demostrar conocimiento de planes confidenciales; objetivos de M&A que sufren incidentes cibernéticos (ej., robo de Propiedad Intelectual).
- Comportamiento inusual de un cliente o *joint venture*: recuerde que es posible que estos no sean siempre clientes o socios legítimos, ya que los criminales cibernéticos pueden integrarse a organizaciones para obtener un acceso más fácil a sus sistemas y datos.
- Conducta inusual de un empleado: los gerentes de personal deben ser más conscientes de los cambios en la conducta, especialmente cuando dicho personal trabaja en áreas sensibles.
- Interrupción operativa pero sin un origen claro.
- Comportamiento anómalo en el procesamiento de pagos y los sistemas de pedidos.
- Bases de datos de clientes o usuarios que muestran información inconsistente.

¿Cuál de las siguientes áreas de seguridad de la información definiría como "prioridades altas, medias o bajas" en los siguientes 12 meses?



56%

de los encuestados define la prevención de la fuga de datos/pérdida de datos como una prioridad alta para su organización durante los siguientes 12 meses.

49%

de los encuestados define los riesgos/amenazas de personal interno como una prioridad media, a pesar de que un 56% dice que los empleados son una de las fuentes más probables de un ataque, y 36% menciona a los contratistas externos como una fuente probable.

50%

de los encuestados define las redes sociales como una prioridad baja.

49%

dice que un incremento de inversión de hasta 25% es necesario para proteger a la organización de acuerdo con la tolerancia al riesgo definida por la gerencia.

¿Por qué debemos estar en "alerta máxima"?

El mundo digital no permite que ninguna organización se sienta cómoda en el área de las amenazas y vulnerabilidades de seguridad cibernética. Es esencial un estado de "alerta máxima" que esté latente, detectando y reaccionando al entorno cambiante. Es necesario considerar un estado de preparación continua, 365 y 24/7.

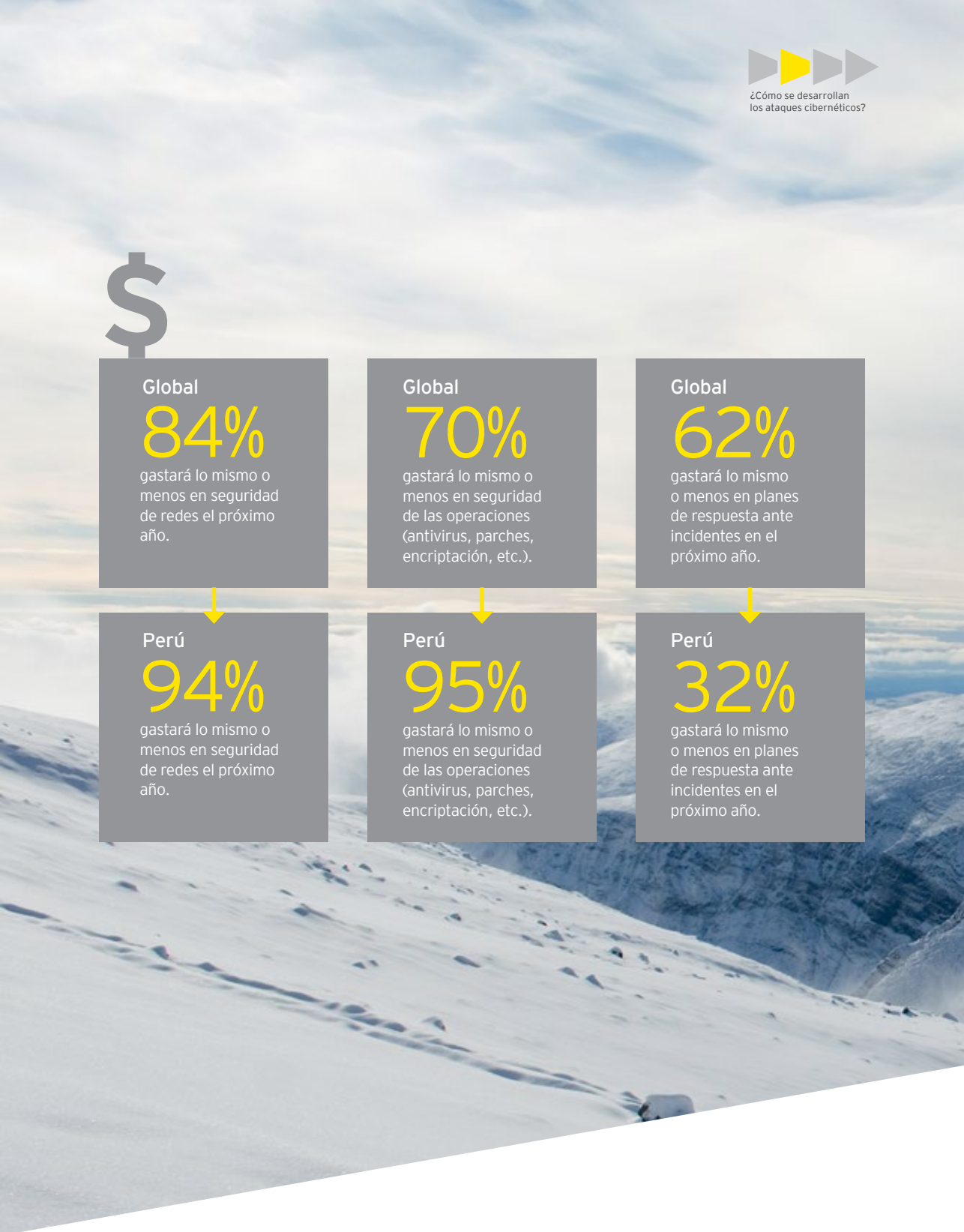
Pero con este grado de alerta o vigilancia, es comprensible que algunas organizaciones se encuentren fatigadas y muchas se pregunten ¿Cuándo será suficiente?.

El bombardeo constante de tres a cuatro años de numerosos ataques y el tener que reaccionar ante eventos cibernéticos puede fácilmente provocar cierto grado de complacencia. Una trayectoria sólida de repeler "ataques típicos" (ej., *phishing*) y el cumplimiento de las brechas obvias (ej., que la Gestión de Identidades y Accesos funcione eficazmente) pueden conducir a las organizaciones a pensar que han "resuelto" el problema de seguridad cibernética, cuando en realidad la situación está empeorando. Esto es especialmente cierto ya que puede ser muy difícil demostrar el valor de la inversión en términos reales cuando los presupuestos están ajustados.

En realidad, la mayoría de las organizaciones han estado implementando las bases para una seguridad cibernética adecuada, sin darse cuenta que esto es sólo el inicio, y el mundo digital requiere de un enfoque de inversión constante. Una organización solo puede considerar que tiene "suficiente" seguridad cibernética cuando la organización es capaz de siempre mantenerse dentro de los límites del apetito de riesgo establecido.

Sin embargo, a medida que aumenta la madurez de seguridad cibernética en una organización, se hace ciertamente más fácil demostrar el valor de estas inversiones. Brindar evaluaciones de pérdidas más exactas sobre el daño que los distintos escenarios de ataques cibernéticos causará, puede ayudar a justificar la inversión y la vigilancia continua. Cada vez que su Centro de Operaciones de Seguridad (COS) o los analistas de inteligencia de amenazas internas identifiquen un ataque en etapas muy tempranas, será posible demostrar el valor de la amenaza extrapolando el daño que habría sido causado si el escenario hubiera resultado ser el peor de los casos.

De manera similar, mientras mejor sea su conocimiento de la situación, más fácil será racionalizar y priorizar su inversión. De esta manera se evitará desperdiciar mucho dinero en controles o equipamiento innecesarios que no mejoran la seguridad cibernética en las áreas donde más se requiere.



Global

84%

gastará lo mismo o menos en seguridad de redes el próximo año.

Perú

94%

gastará lo mismo o menos en seguridad de redes el próximo año.

Global

70%

gastará lo mismo o menos en seguridad de las operaciones (antivirus, parches, encriptación, etc.).

Perú

95%

gastará lo mismo o menos en seguridad de las operaciones (antivirus, parches, encriptación, etc.).

Global

62%

gastará lo mismo o menos en planes de respuesta ante incidentes en el próximo año.

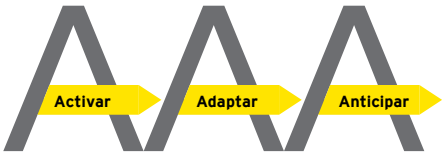
Perú

32%

gastará lo mismo o menos en planes de respuesta ante incidentes en el próximo año.

¿Por qué seguimos siendo tan vulnerables?

En nuestra encuesta Global de Seguridad del 2014, identificamos tres etapas de madurez de seguridad cibernética: Activar, Adaptar y Anticipar (las tres As) que necesitan ejecutarse en secuencia con el fin de lograr medidas de seguridad cibernética cada vez más avanzadas e integrales en cada etapa.



Las tres As siguen siendo relevantes, y los resultados de nuestra encuesta del 2015 muestran que aún quedan avances por realizar en las tres etapas. Sin embargo, frente a las amenazas de hoy en día, muchas de las acciones que hemos identificado como acciones más avanzadas se han vuelto ahora fundamentales.

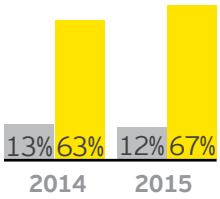
1. Activar

Es aquí donde una organización logra una base sólida en materia de seguridad cibernética para su entorno actual, la cual comprende un conjunto de medidas de seguridad cibernética que ayudan a proporcionar una defensa básica. Se requiere que la organización:

- Realice una evaluación de seguridad y cree una hoja de ruta.
- Obtenga el respaldo a nivel del Directorio para una transformación de la gestión de seguridad.
- Revise y actualice las políticas de seguridad, los procedimientos y normas de soporte.
- Establezca un Centro de Operaciones de Seguridad (COS).
- Pruebe los planes de continuidad del negocio y procedimientos de respuesta ante incidentes.
- Diseñe e implemente controles de seguridad cibernética.

Hoy en día, con los riesgos y amenazas cibernéticas cada vez más sofisticadas, existen dos tareas fundamentales adicionales:

- Definir el entorno de la organización.
- Introducir la capacitación y concientización en seguridad cibernética a los empleados.



Porcentaje de los encuestados que considera que su función de seguridad de la información cumple completamente con las necesidades de su organización.

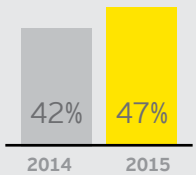
Porcentaje de los encuestados que considera que cumple parcialmente con las necesidades de su organización.

¿Entonces, dónde estamos en el 2015?

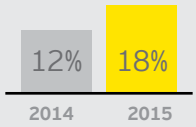
No es suficiente lo realizado a la fecha

Sólo el 12% piensa ahora que su función de Seguridad de la Información cumple plenamente con las necesidades de la organización. Un 67% se encuentra todavía realizando mejoras.

- Se presenta una caída del 1% entre aquellos que piensa que las necesidades se están cumpliendo plenamente, pero la cantidad de encuestados que están realizando mejoras ha aumentado solo en un 4% desde 2014.
- 69% dice que su presupuesto de seguridad de la información necesita incrementarse hasta un 50% para proteger a la empresa de acuerdo con la tolerancia del riesgo establecida por la gerencia.
- 47% no tiene un COS establecido, comparado con 42% en el año 2014.
- 37% no tiene un esquema de protección de datos, o sólo tiene políticas o procesos *"ad hoc"* implementados, comparado con 34% en el 2014.
- 18% no tiene un programa de Gestión de Identidades y Accesos, mientras que en el 2014 esta cifra era solo de 12%, lo cual representa una caída considerable.
- Solo un 42% posee un inventario exacto de su entorno (es decir, todos los proveedores terceros, conexiones a la red y datos).
- 27% dice que el *phishing* dirigido a usuarios finales fue la principal falla de control o proceso que condujo a una violación cibernética considerable en este último año.



Porcentaje de encuestados que no cuenta con un COS.



Porcentaje de encuestados que no cuenta con un programa de Gestión de Identidad y Accesos.

54%

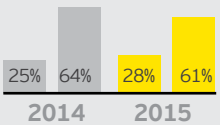
de las organizaciones en la actualidad no tiene un rol o un departamento en su función de seguridad de la información que se centre en la tecnología emergente y su impacto en la organización.

2. Adaptar

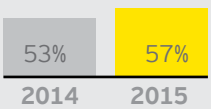
Al entender que las medidas fundamentales de seguridad de la información se volverán menos eficaces con el tiempo, en esta etapa nos enfocamos en el entorno cambiante y destacamos las acciones necesarias para asegurar que las organizaciones puedan seguir adaptándose para ajustarse al ritmo y responder a los cambiantes requisitos y a las dinámicas empresariales.

Hoy en día, la etapa de Adaptación requiere lo siguiente:

- Diseñar e implementar un programa de transformación para lograr una mejora en la madurez de la seguridad cibernética, utilizando apoyo externo para acelerar o incorporar las prácticas de vanguardia en el diseño y gestión del programa.
- Decidir qué mantener internamente y qué tercerizar.
- Definir una matriz RACI (Responsable, Aprobador, Consultado, Informado) para la seguridad cibernética.



Porcentaje de encuestados que tiene la intención de invertir más en la transformación de la seguridad de la información versus los que invierten lo mismo.



Porcentaje que dice que la falta de recursos calificados está desafiando la contribución y el valor de la seguridad de la información en la organización.

¿Entonces, dónde estamos en el 2015?

No hay suficiente adaptación al cambio

- El 54% de las organizaciones no tiene actualmente un rol o departamento en su función de seguridad de la información que se centre en la tecnología emergente y su impacto – esto incluye un 36% que no tiene planes para implementarlos.
- Sólo el 34% calificaría a su monitoreo de la seguridad como maduro o muy maduro, lo cual es sólo un aumento del 4% con respecto al 2014.
- Sólo el 53% calificaría a su seguridad de la red como maduro o muy maduro, lo cual es sólo un aumento del 1% con respecto al 2014.
- El 57% dice que la falta de recursos calificados está desafiando la contribución y el valor de la seguridad de la información a la organización, mientras que en el 2014 esta cifra fue 53%.
- Cuando se les preguntó "en comparación con el año anterior," el 28% de los encuestados dijeron que planeaban invertir más en la transformación de la seguridad de la información (un rediseño fundamental); esto es sólo un aumento del 3% en las respuestas a la misma pregunta en el 2014.

3. Anticipar

En la etapa Anticipar, una organización tiene que desarrollar de manera proactiva tácticas para detectar y neutralizar posibles ataques cibernéticos. Debe centrarse en el entorno futuro y tener más confianza en su capacidad para manejar amenazas más predecibles, así como ataques inesperados.

Pocas organizaciones están en este nivel, y en la actualidad se requiere que estas:

- Diseñen e implementen una estrategia de análisis de inteligencia sobre amenazas cibernéticas.
- Definan y abarquen el entorno extendido de seguridad cibernética de la organización.
- Adopten un enfoque económico cibernético.
- Utilicen *Data Analytics Forenses* y el análisis de inteligencia sobre amenazas cibernéticas.
- Se aseguren de que todos entiendan lo que está pasando.
- Se preparen para lo peor mediante el desarrollo de una estrategia de gestión de respuesta ante ataques cibernéticos.

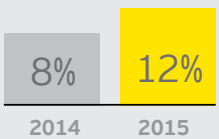
36%

de los encuestados no tiene un programa de análisis de inteligencia sobre amenazas.

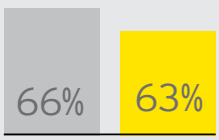
¿Entonces, dónde estamos en el 2015?

Enfoque lento para enfrentar los ataques cibernéticos sofisticados

- El 36% no cuenta con un programa de análisis de inteligencia sobre amenazas, con otro 30% que sólo tiene un enfoque informal, mientras que el 5% dice que su organización ha logrado una función avanzada de inteligencia sobre amenazas; en comparación con el 2014, estas cifras no han cambiado, a no ser por un descenso del 2% en los que tienen el enfoque informal.
- El 63% dice que la gestión de las amenazas y las vulnerabilidades es una prioridad media o baja, lo cual es sólo una mejora con respecto al 2014.
- Sólo el 12% mira más allá de sus proveedores, hacia los proveedores de sus proveedores (cuartas partes), lo cual es sólo una mejora del 4% con respecto al 2014.
- Sólo el 31% de todos los terceros tiene una clasificación apropiada de riesgo y diligencia en su operación, en comparación con el 27% en 2014.
- El 79% dice que el mal comportamiento del usuario es el principal riesgo asociado con los dispositivos móviles.



Porcentaje de encuestados que está atento a los proveedores de sus proveedores.

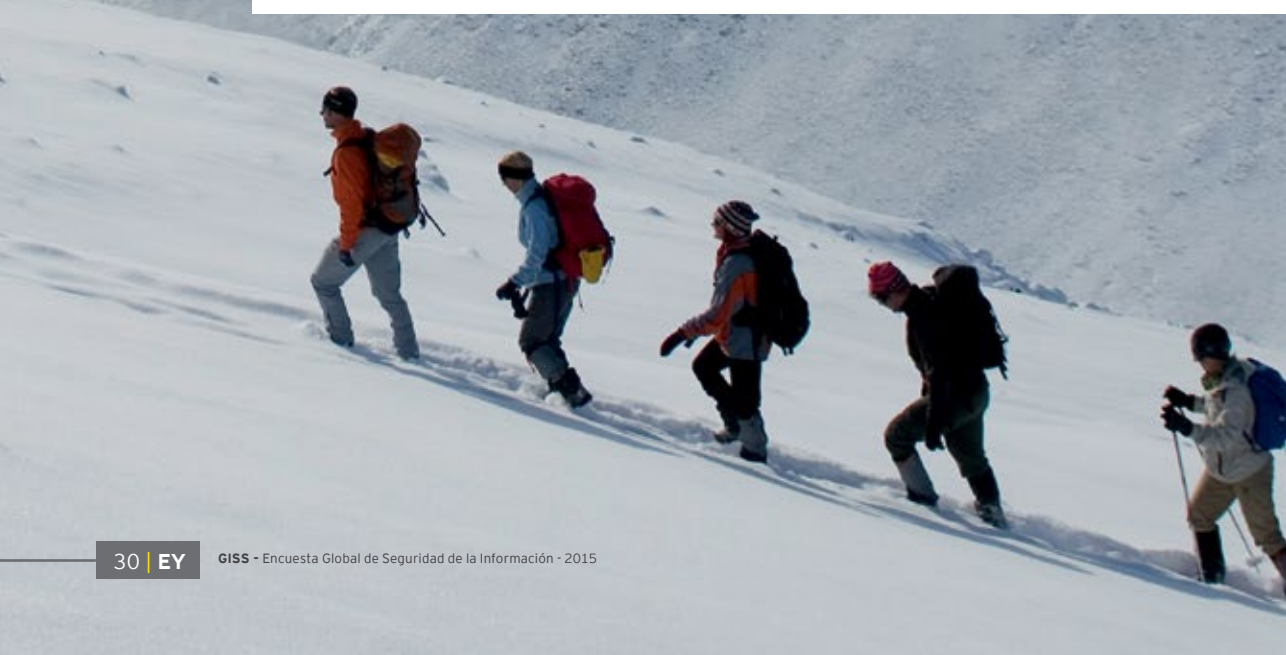


Porcentaje de encuestados que dice que la gestión de las amenazas y la vulnerabilidades es una prioridad media o baja.

El cambio hacia una Defensa Activa

¿Qué es la Defensa Activa?

La seguridad cibernética es una capacidad inherente de defensa para las organizaciones. Los departamentos de defensa de los gobiernos (y el ejército) pueden estar preparando capacidades ofensivas, desarrollando armas cibernéticas y realizando actividades de intrusión, pero para las organizaciones fuera de ese estrecho ámbito, las operaciones ofensivas siguen siendo consideradas como innecesarias y se presentan a menudo en una "zona gris".



Sin embargo, eso no quiere decir que las organizaciones tienen que ser pasivas y esperar a convertirse en víctimas.

Como se ha descrito anteriormente en el presente documento, comprender los riesgos cibernéticos críticos de la empresa y saber lo que los atacantes podrían desear de la organización,les permite establecer una "defensa dirigida" a través de la priorización (de activos, personas, áreas de negocio) y el refuerzo de sus vulnerabilidades. Evaluar el entorno de las amenazas de su organización (en función de su entorno operativo, activos críticos y estrategia de negocio) le permite comprender a los protagonistas de estas amenazas y los métodos más probables que estos pueden utilizar. Todo esto deberá ser informado por su COS y debe ser la base sobre la cual este apoyará a su organización.

Implementar un COS más avanzado y utilizar el análisis de inteligencia sobre las Amenazas Cibernéticas para alinearlas con eficacia en las operaciones, permite llevar a cabo una Defensa Activa mediante el envío de alertas inteligentes para buscar posibles atacantes, evaluar la amenaza, y neutralizarla antes de que pueda dañar los activos críticos de su organización. Del mismo modo, usted puede utilizar un COS avanzado para operar e identificar a los "visitantes" o atacantes que ya estén en sus sistemas.

Global

24%

Perú

91%

de los encuestados no tiene un programa de identificación de vulnerabilidades.

¿Qué debemos mejorar?

Inteligencia Avanzada sobre Amenazas Cibernéticas: ahora se pueden llevar a cabo en diferentes niveles de evaluación de amenazas y perfiles, escalando a partir de las preguntas más básicas. La Inteligencia más Avanzada sobre Amenazas Cibernéticas le permite gestionar de forma proactiva estas amenazas y las medidas de protección.

¿Necesita mejorar su análisis de Inteligencia sobre Amenazas Cibernéticas?

Global

34%

Perú

6%

tiene un programa *"ad hoc"* de identificación de vulnerabilidades y realizan pruebas automatizadas con regularidad.

Global

27%

dice que tienen implementadas políticas y procedimientos *"ad hoc"* de protección de datos.

Preguntas claves para su encargado de seguridad de la información:

- ¿Qué información sobre mi organización/compañía está disponible para un atacante? ¿Cómo podrían utilizarla?
- ¿Qué tipo de atacantes son mis adversarios más probables (ej., *hacktivistas*, redes criminales en busca de cosas para vender, estafadores?
- ¿Cuáles son sus capacidades (ej., recursos probables, cronograma, capacidades técnicas, capacidad de reclutar personas internas de la empresa)?
- Para cada uno de los adversarios más probables, ¿en qué estarán interesados? (Compare esto con su lista de lo que realmente importa más en su organización/compañía – sus "joyas de la corona.")
- ¿Cuán vulnerables son estos objetivos/activos deseados, y cómo podrían ser explotados?
- ¿Qué caminos específicos podrían tomar los adversarios hasta su objetivo deseado (ej., a través de un sistema de aire acondicionado, a través de un sistema de pago, reclutando a una persona interna a la empresa, utilizando el *spear-phishing* ante miembros del Directorio o empleados designados que tienen acceso)?
- ¿Cuáles son las medidas de protección más eficaces?
- ¿Qué más puedo aprender de los incidentes previos con adversarios o atacantes?

Con las respuestas, una organización podría utilizar los hallazgos para tomar decisiones estratégicas e informarlas a nivel ejecutivo y re-enfocar la actividad operativa en el COS.

¿Cómo implementar la Defensa Activa?

La Defensa Activa amplía la capacidad tradicional de las operaciones de seguridad de dos maneras: Primero debe ser guiada por un análisis de inteligencia sobre Amenazas Cibernéticas. Más que solo recibir "fuentes de información", el análisis real de la inteligencia sobre amenazas permite a los profesionales de la Defensa Activa identificar probables atacantes, inferir sus objetivos más probables dentro de su empresa, y desarrollar hipótesis acerca de las formas probables en que esos ataques se desarrollarán. Este entendimiento permite la implementación de medidas de protección a medida.

El segundo diferenciador clave con respecto al enfoque de seguridad cibernética es el ciclo operativo de la Defensa Activa. Para analizar la información disponible y sacar conclusiones relevantes, los profesionales de la Defensa Activa deberían utilizar un proceso definido y disciplinado, el cual puede añadir un componente dinámico y proactivo a las operaciones de seguridad existentes en la organización.

A diferencia de otros ofrecimientos de servicios de seguridad, la Defensa Activa no tiene por objetivo mejorar un área funcional específica o implementar nuevas tecnologías. En vez de ello, la Defensa Activa integra y analiza las capacidades de seguridad existentes de la empresa para lograr una mayor eficacia contra los atacantes persistentes. Mediante la implementación y ejecución de un ciclo iterativo con mecanismos incorporados para el aprendizaje y la mejora continua, la organización puede obtener ganancias en las capacidades de eficiencia, rendición de cuentas y gobierno. Estas ganancias se traducen directamente en un retorno sobre la inversión donde aumenta la eficacia de las operaciones de seguridad y a su vez, reducen la eficacia de los ataques dirigidos.

La Defensa Activa también debe incluir la evaluación de las implicancias de riesgo en el caso de un ataque cibernético grave y el desarrollo de un marco de respuesta centralizado como parte de la estrategia de gestión de riesgos de la empresa. El marco de gestión de respuesta ante un ataque cibernético, con un modelo de gobierno claramente definido, debe cubrir el proceso de investigación de incidentes, recopilación y análisis de pruebas, evaluación del impacto y soporte ante litigios.

Global

59%

de los encuestados dice que su COS posee una suscripción pagada a fuentes de información de inteligencia sobre amenazas cibernética.

Global

66%

Perú

6%

porcentaje de encuestados que habían tenido recientemente un incidente significativo de seguridad cibernética que no fue descubierto por su COS, y dice que su COS no tiene una suscripción pagada a las fuentes de información de inteligencia sobre amenazas cibernéticas.

¿Es la Defensa Activa apropiada para su organización?

Si la respuesta a cualquiera de las siguientes preguntas es "sí", usted debe considerar un enfoque de Defensa Activa:

- No contamos con un COS implementado. Actualmente tenemos controles de seguridad clásicos.
- Tenemos un COS, pero todavía no hemos encontrado pruebas de atacantes avanzados.
- Tenemos un COS, pero sin embargo tuvimos un incidente mayor.
- Tenemos un COS tercerizado, pero nuestros sistemas de propiedad intelectual y comerciales no están verdaderamente seguros.

Los próximos pasos hacia el desarrollo de un entorno digital confiable.

¿Qué necesita mi organización?:

- Conocimiento de lo que puede perjudicar a la organización y perturbar el logro de su estrategia.
- Identificación clara de sus activos críticos.
- Escenarios de riesgo cibernético que muestren un esquema exacto de cómo podría desencadenarse un ataque.
- El Directorio y los altos ejecutivos puedan determinar con precisión el apetito de riesgo para la organización.

- Una evaluación del nivel de madurez actual de la seguridad cibernética y una comparación con el nivel de madurez que se requiere realmente para satisfacer el apetito de riesgo.
- Una hoja de ruta de mejora en ciberseguridad.
- Elaboración de escenarios de amenazas y un análisis de inteligencia avanzado sobre los mismos.
- Un COS más avanzado: interno, en tercerización conjunta (co-sourced) o tercerizado por completo.
- Una estrategia proactiva y multifuncional para la gestión de la respuesta a los incidentes cibernéticos.

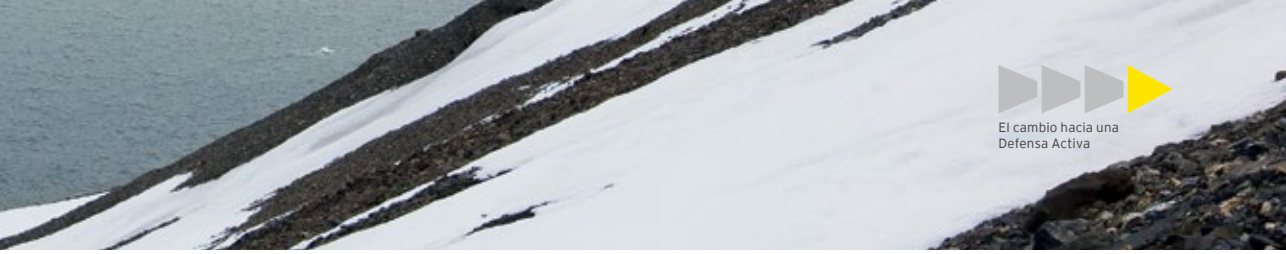
El avance en la hoja de ruta de seguridad cibernética y en el plan de implementación podría requerir un cambio cultural en su organización y claridad en torno al rol del Directorio.

Es probable que sean necesarios recursos externos para ayudar a su organización a lograrlo. Actualmente, una evaluación a nivel del Directorio podría ser un ejercicio inicial y muy eficaz para preparar el terreno para la magnitud de cambios que podrían ser necesarios.

Las páginas siguientes ofrecen el espectro completo de los estados de madurez — ¿dónde se encuentra ahora, y dónde cree que necesita estar? El enfoque de defensa dirigida no sugiere que el estado ideal sea esencial en todos los aspectos.

El análisis de madurez — y dónde figuran las organizaciones actualmente

Pregunta sobre la madurez	1 — No-existente	2
¿Cuál es la madurez de su programa de inteligencia sobre amenazas?	El **35%** de los encuestados no tiene un programa de inteligencia sobre amenazas.	El **30%** tiene un programa informal de inteligencia sobre amenazas que incorpora información confiable de terceros, y listas de distribución de correo electrónico.
¿Cuál es el nivel de madurez de su capacidad de identificación de vulnerabilidades?	El **24%** de los encuestados no tiene un programa de identificación de vulnerabilidades.	El **33%** tiene un programa informal de identificación de vulnerabilidades y lleva a cabo pruebas automatizadas con regularidad.
¿Cuál es el nivel de madurez de su programa de detección de incidentes?	El **17%** de los encuestados no tiene un programa de detección de incidentes; otro **4%** no tiene procesos formales implementados para la respuesta y el escalamiento.	El **22%** tiene dispositivos perimétricos de seguridad de redes (es decir, IDS); otro **20%** utiliza una solución de Gestión de la Información y Eventos de Seguridad (SIEM) para monitorear activamente la red, IDS/IPS y los registros del sistema.



3	4	5 – Muy madura
El **20%** tiene un programa formal de análisis de inteligencia sobre amenazas que incluye la suscripción a fuentes de información sobre amenazas de proveedores externos y fuentes internas, tales como la herramienta de gestión de incidentes y eventos de seguridad.	El **10%** tiene un equipo de inteligencia sobre amenazas que recopila fuentes de información de amenaza y vulnerabilidad internos y externos para analizar y determinar la credibilidad y relevancia en su entorno.	El **5%** tiene una función avanzada de análisis de inteligencia sobre amenazas con fuentes de información internos y externos y analistas de inteligencia dedicados, y asesores externos que evalúan la información para determinar la credibilidad, relevancia y exposición a las amenazas.
El **20%** utiliza una variedad de enfoques de estudio, incluyendo la ingeniería social y pruebas manuales.	El **18%** tiene una función formal de inteligencia de análisis sobre vulnerabilidades con un programa de evaluaciones de amenazas utilizando ataques en profundidad y pruebas de penetración de proveedores, pruebas periódicas de procesos empresariales y pruebas de proyectos (ej., nuevos sistemas).	El **5%** tiene una función avanzada de inteligencia de análisis sobre vulnerabilidadesy lleva a cabo evaluaciones de riesgo con resultados y soluciones acordes con la función de riesgo durante todo el año.
El **6%** tiene procesos informales de respuesta y escalamiento implementados; otro **5%** utiliza procesos ad hoc para la recopilación, integración, respuesta y escalada de amenazas.	El **13%** tiene un programa formal de detección que aprovecha las tecnologías modernas (detección de *malware* basada en el host y basada en la red, detección de anomalías de comportamiento, etc.) para monitorear tanto el tráfico interno como externo.	El **11%** tiene una función formal y avanzada de detección que reúne a cada categoría de la tecnología moderna (detección de *malware* basada en el *host*, antivirus, detección de *malware* basada en la red, DLP, IDS, cortafuegos de próxima generación, agregación de registros) y hace uso del análisis de datos sofisticados para identificar anomalías, tendencias y correlaciones. Sin embargo, sólo el **2%** tiene procesos formales para la recolección de amenazas, la difusión, integración, respuesta, escalamiento y predicción de los ataques.

Pregunta sobre la madurez	1 – No-existente	2
¿Cuál es el nivel de madurez de la capacidad de respuesta a incidentes de computadora?	El **14%** no cuenta con una capacidad de respuesta ante incidentes.	El **21%** tiene un plan de respuesta ante incidentes a través del cual pueden recuperarse de *malware* y la mala conducta de los empleados; no se realizan más investigaciones sobre las causas raíces.
¿Cuál es la madurez de su programa de protección de datos?	El **10%** de los encuestados no tiene un programa de protección de datos.	El **27%** dice que las políticas y procedimientos de protección de datos son informales o que tienen implementadas políticas ad hoc .
¿Cuál es la madurez de su gestión de identidad y acceso?	El **18%** de los encuestados no tiene un programa de gestión de identidades y acceso.	El **25%** tiene un equipo que supervisa los procesos de gestión de acceso y el repositorio central; la realización de estudios no está establecida formalmente.

3	4	5 – Muy madura
El **43%** tiene un programa formal de respuesta ante incidentes y lleva a cabo investigaciones tras un incidente.	El **16%** tiene un programa formal de respuesta ante incidentes y acuerdos establecidos con vendedores externos para servicios e investigaciones de respuesta más completos en temas de identidad.	El **7%** tiene un programa sólido de respuesta a incidentes que incluye a terceros y las fuerzas del orden y se integra con su función más amplia de gestión de amenazas y vulnerabilidades; también elaboran libros de estrategias para incidentes potenciales y los prueban a través de ejercicios de simulación en escritorio con regularidad.
El **19%** dice que las políticas y los procedimientos de protección de datos están definidos a nivel de unidad de negocio.	El **26%** dice que las políticas y los procedimientos de protección de datos están definidos a nivel de grupo.	El **17%** dice que las políticas y los procedimientos de protección de datos están definidos a nivel de grupo, reflejando la supervisión corporativa y siendo comunicados a toda la empresa; las excepciones específicas de las unidades de negocio están documentadas y son monitoreadas y revisadas anualmente.
El **34%** tiene un equipo formal para supervisar los procesos de gestión de acceso definidos, aunque esto sea en gran parte manual; un Directorio central ha sido implementado, sin embargo interactúa con un número limitado de aplicaciones y no se revisa periódicamente.		El **23%** tiene un equipo formal que interactúa con las unidades de negocio para la obtención de supervisión IAM*; tienen procesos bien definidos, flujos de trabajo automatizados limitados, conexión del usuario fuente de única para la mayoría de aplicaciones y realizan revisiones periódicas.

* Identity & Access Management

Global

32%

Perú

89%

de encuestados indicó que hacer el *benchmarking* de la información acerca de la madurez de las organizaciones pares fue lo más útil y de más alta prioridad.

Encamine a su organización hacia la mejora continua

Pocas organizaciones tienen hoy en día las habilidades y recursos apropiados internamente para proteger eficazmente sus activos de información y al mismo tiempo optimizar el desempeño empresarial. Las organizaciones en todos los sectores pueden beneficiarse de una evaluación objetiva de sus programas y estructuras de seguridad de la información.

Una evaluación eficaz debe buscar ayudar a su organización a:

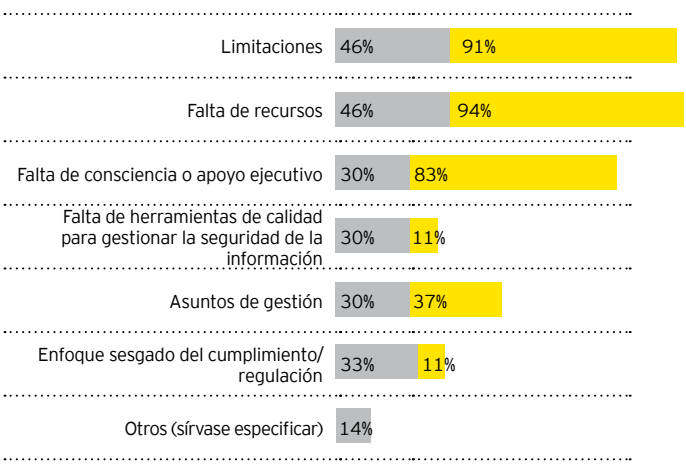
- Comprender la exposición al riesgo de su organización.
- Evaluar la madurez de su programa de seguridad cibernética actual e identificar áreas para su mejora.
- Crear una hoja de ruta priorizada para las inversiones en proyectos e iniciativas de cambio organizacional.
- Recopilar información para crear *benchmarks* con respecto a otras organizaciones.
- Validar el hecho de que sus inversiones en seguridad han mejorado su posición en seguridad.

Esta evaluación necesita ser amplia y de alto nivel, que contemple las áreas y componentes específicos, y aquí es donde EY puede apoyarlo. Las métricas de tablero permite que una organización vea lo que es necesario apoyar en la evaluación.

En la siguiente página se muestra un ejemplo de clasificaciones de madurez que pueden ayudar a posicionar a la organización en el espectro relevante para su estado actual, competitivo y futuro.

La eficacia de la seguridad de la información

¿Cuáles son los principales obstáculos o razones que son un desafío para la contribución y entrega de valor a la organización por parte de la seguridad de la información?



¿Tiene usted una matriz RACI?

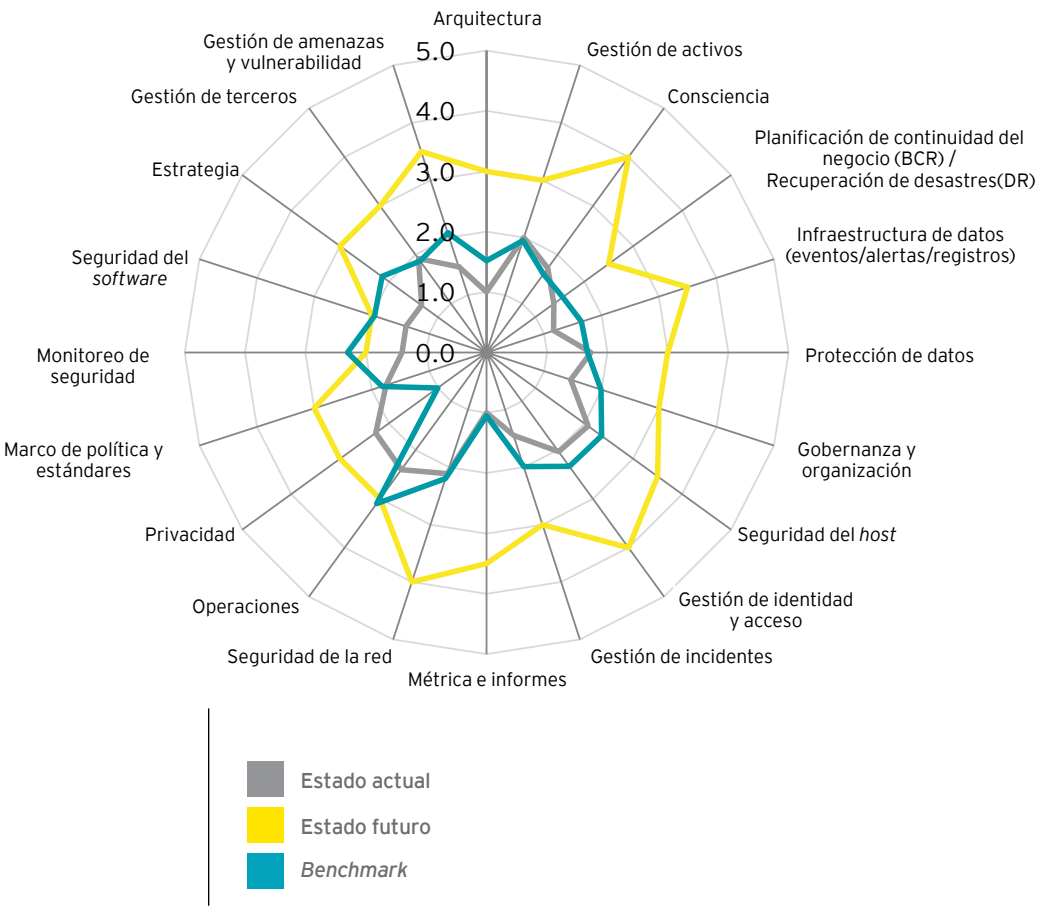
Debido a que el Directorio establece el tono y el nivel de expectativa, la colaboración de toda la empresa es esencial, así como la vigilancia relativa de "cómo los riesgos y ataques cibernéticos afectan su rol". Una gestión de seguridad eficaz afecta cada rol y cada parte de la organización; una matriz RACI, una buena gobernanza y empleados solidarios son todos esenciales para nuestro enfoque 3 As. Considere qué aspecto debe tener una matriz RACI para su organización, y tenga claro que la seguridad cibernética ya no es solamente un tema de TI.

Comparación del estado actual de madurez de la seguridad cibernética entre la organización X y sus pares.

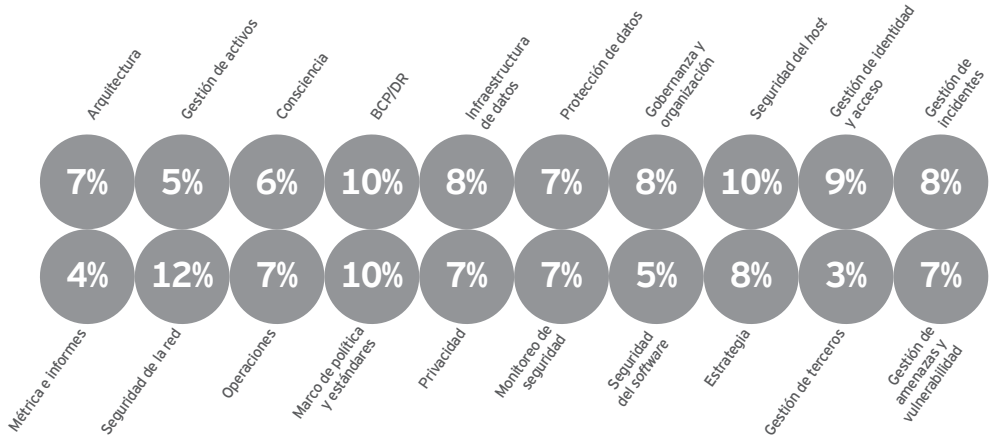
El nivel de madurez actual de X está aproximadamente en el mismo nivel que el de pares comparables.

El estado futuro definido aumenta considerablemente el nivel de madurez.

Organización X versus sus pares



El porcentaje de encuestados que indicaron que su nivel de madurez era "muy maduro"



La seguridad cibernética no es un inhibidor del mundo digital; más bien, ayuda a hacer que el mundo digital se mantenga totalmente operativo y sostenible.

La seguridad cibernética es clave para adoptar la innovación y la diversificación. Adoptando una organización enfocada en los riesgos de la seguridad cibernética, las organizaciones pueden re-enfocarse en las oportunidades y en la exploración de nuevas iniciativas. Desarrollar el nivel de confianza en una empresa que opera exitosamente en Internet o "en línea", y que apoya y protege plenamente a las personas y sus dispositivos móviles personales (desde un simple teléfono hasta un dispositivo de cuidado de la salud, desde dispositivos inteligentes hasta carros inteligentes), es clave para obtener un diferenciador competitivo y debe ser una prioridad.

Si actuamos ahora, es posible lograr un equilibrio en el mundo digital hacia la sostenibilidad y la seguridad, para ayudar a proteger mejor su organización y crear confianza en su marca.

Metodología de la **Encuesta Global de Seguridad de la Información**

La Encuesta Global de Seguridad de la Información de EY se realizó entre junio y setiembre de 2015. Los participantes incluyeron 1,755 encuestados de 67 países y de las industrias de mayor importancia.

Para nuestra encuesta, invitamos a participar a CIOs, CISOs, CFOs, CEOs y otros ejecutivos de seguridad de la información. Distribuimos un cuestionario a los profesionales de EY designados en la práctica de cada país, junto con instrucciones para la administración consistente del proceso de encuesta.

La mayoría de respuestas de la encuesta fueron recolectadas durante entrevistas personales. Cuando esto no fue posible, el cuestionario fue llenado en línea.

Si usted desea participar en futuras Encuestas Globales de Seguridad de la Información de EY, sírvase contactar a su representante de EY o su oficina local, o visite www.ey.com/giss y llene un simple formulario de solicitud.

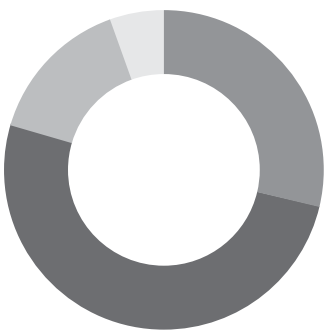
Perfil de los participantes

1,755
encuestados

25
sectores de la industria

67
países a nivel mundial

Encuestados por área (1,755 respuestas)

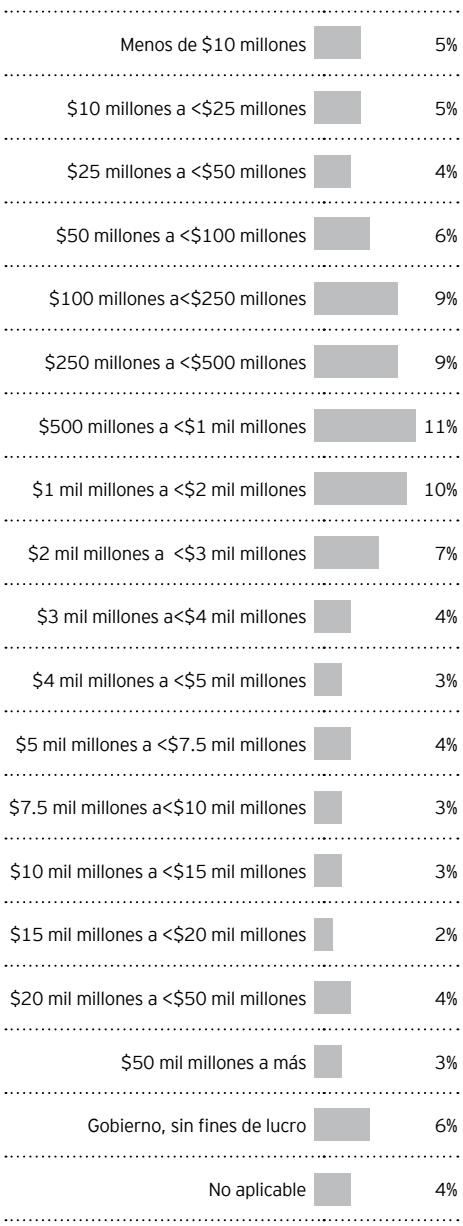


Key:

- EMEIA 51%
- Américas 29%
- Asia-Pacífico 15%
- Japón 5%

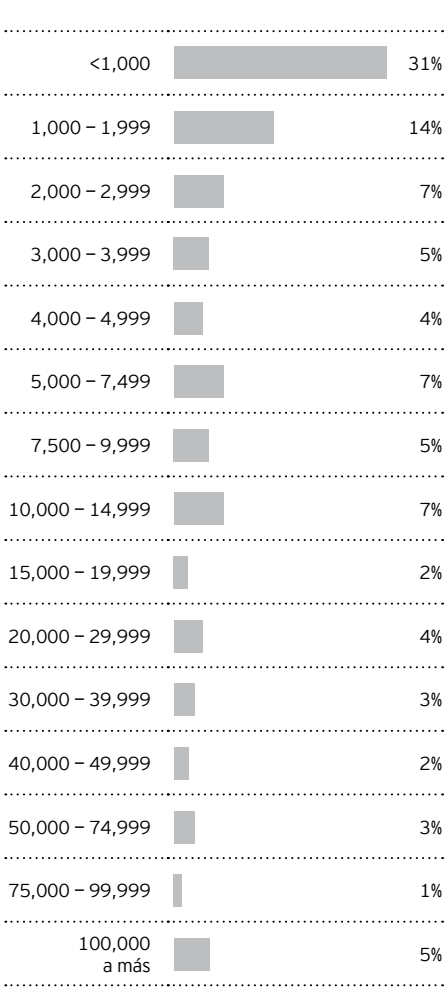
Encuestados por ingresos anuales totales en sus organizaciones

todos los montos son en dólares americanos

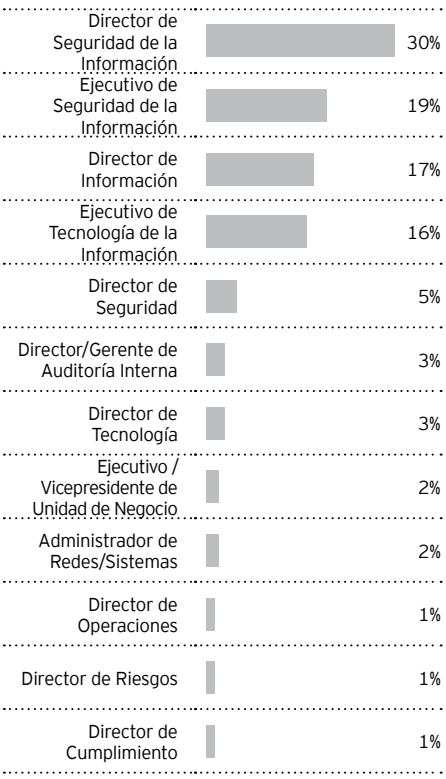


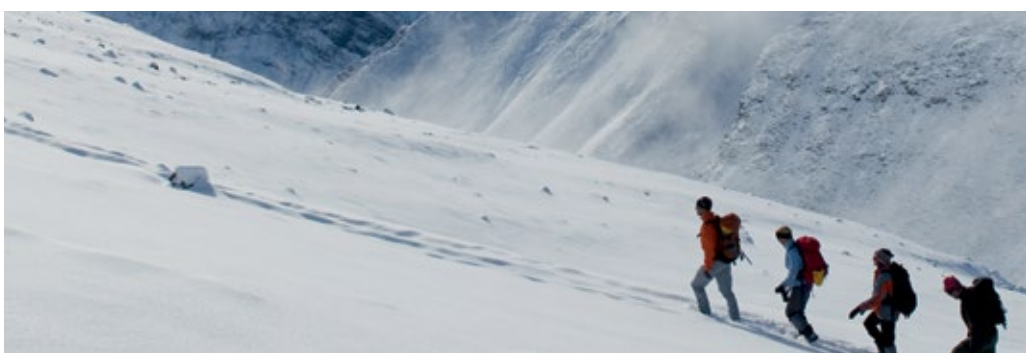
Encuestados por sector

Encuestados por número de empleados



Encuestados por cargo





Anexos

Anexo 01

Optimizando sus operaciones de seguridad con una **Defensa Activa**

Los siguientes pasos de mejora continua

Los profesionales en operaciones de seguridad han visto los títulares y han leído los informes de los ataques cibernéticos que se vuelven más sofisticados y destructivos. De acuerdo con las tendencias identificadas por la última Encuesta Global de Seguridad de la Información de EY, la mayoría de las organizaciones está luchando para ajustarse a esta evolución. Nuestra encuesta de 2014 indicó que el 49% de encuestados preveía que sus presupuestos de seguridad se mantendrían "más o menos igual". Aunque en nuestra encuesta de 2015 esta cifra disminuyó a 39%, el porcentaje de las organizaciones que reportaron planes para aumentar los gastos en 5%-25% creció en apenas 4%. Muchos equipos de seguridad enfrentarán otro año con los mismos o menos recursos de los que tuvieron el año que pasó.

Ser capaz de desplegar efectivamente los recursos de seguridad que se han asignado también puede ser un desafío para una organización. 71% de los encuestados estimó la probabilidad de que su organización detectara un ataque cibernético sofisticado en menos del 50%. El obstáculo más común citado para la eficacia del programa de seguridad fue las "limitaciones presupuestarias", con 62%, y la "falta de recursos calificados" muy cerca detrás, con 57%. El efecto acumulativo de todas estas dificultades está bien documentado: el tiempo promedio transcurrido entre la ocurrencia de la violación y el descubrimiento de la misma es de 205 días!

88%

de las funciones de Seguridad de la Información no cumplen plenamente las necesidades organizacionales.

11%

de encuestados del GISS reportó utilizar data analytics para detectar ataques de seguridad.

¿Cómo pueden mejorar las organizaciones? La respuesta es contar con una Defensa Activa.

Los siguientes cuatro capítulos del presente anexo presentarán la perspectiva de EY sobre la Defensa Activa y mostrarán cómo su organización podría adoptarla para ayudar a mejorar su seguridad cibernética:

¿Qué es la Defensa Activa?

- La Visión de EY de la Defensa Activa.
- ¿Qué agrega la Defensa Activa al programa de operaciones de seguridad existente?
- ¿Cómo encaja la Defensa Activa en un programa de seguridad cibernética?

Preparar una Defensa Activa

- ¿Cuáles son los prerrequisitos para establecer un programa de Defensa Activa?
- ¿Qué debo comprender sobre mi organización para habilitar la Defensa Activa?
- ¿Qué debo comprender sobre mis adversarios para que una Defensa Activa sea exitosa?

Realizar una Defensa Activa

- ¿Cuáles son los componentes de una Defensa Activa?
- ¿Qué es una misión de Defensa Activa?
- ¿Qué tipos de misiones puedo realizar con la Defensa Activa?

¿La Defensa Activa es adecuada para mi organización?

- ¿Cuáles son los beneficios de poseer una Defensa Activa?
- ¿Está mi organización lista para implementar una Defensa Activa?
- ¿Cómo puede EY ayudarme a prepararme para realizar una Defensa Activa en el futuro?

¿Qué es la Defensa Activa?

Para entender cómo la Defensa Activa puede ayudar a mejorar la eficacia del programa de seguridad, necesitamos una analogía. Muchas organizaciones piensan que la red ideal de una empresa es como un castillo o una fortaleza: este modelo mental incluye muros gruesos de piedra, torres de guardia y quizás incluso un foso. Los castillos podrán mantener lejos a los invasores del mundo real, pero hemos aprendido una y otra vez que los atacantes casi siempre tienen éxito en penetrar incluso las redes más seguras a través de ataques dirigidos. Los profesionales de seguridad no pueden confiar en la integridad del perímetro de la red y deben operar bajo el supuesto de que actividades maliciosas no detectadas están presentes casi todo el tiempo.

Una analogía más apropiada podría ser la red de la empresa como una ciudad contemporánea. Esta analogía funciona en varios niveles. Considere las formas evolutivas que utilizamos para acceder a los datos. Los usuarios tienen múltiples rutas para entrar y salir de la red a través de las estaciones de trabajo de la empresa, dispositivos móviles propios, almacenamiento en nube y más. Esto significa que, tanto los usuarios legítimos, como los intrusos, tienen numerosas oportunidades para realizar actividades que no se ven. Así como cualquier ciudad de tamaño suficiente vive actividades criminales casi constantes sin vigilancia policial, los tamaños y la complejidad en expansión de las redes también han afectado la capacidad de los defensores para monitorearlas en tiempo real. De hecho, los participantes que, en la Encuesta Global de Seguridad 2015 de EY, reportaron haber vivido incidentes significativos, revelaron que sólo el 45% de los incidentes detectados fueron descubiertos por el Centro de Operaciones de Seguridad (COS). Para mantener el orden, los guardias de castillo de antaño evolucionaron para convertirse en la policía moderna, y los profesionales de las operaciones de seguridad deben evolucionar también.

La defensa activa es una campaña planificada y ejecutada continuamente para identificar y ayudar a erradicar a los atacantes ocultos y vencer posibles escenarios de amenaza dirigidos a sus activos más fundamentales.

¿Qué agrega la Defensa Activa al programa de operaciones de seguridad existente?

Llevemos nuestra analogía al COS. El equipo de operaciones de seguridad conforma la fuerza policial de la red de la empresa. El monitoreo de seguridad con las herramientas de red es como enviar a oficiales al exterior para hacer cumplir los límites de velocidad y vigilar el crimen. En el mundo real, los oficiales de patrulla son eficaces para disuadir y vencer a los criminales que pueden realmente

ver. Sin embargo, no son eficaces para vencer el crimen sofisticado que se produce a puerta cerrada y en áreas que no son patrulladas. Para esto, la ciudad necesita detectives. En lugar de patrullar y monitorear, los detectives tienen informantes, investigan pistas, analizan pruebas y activamente buscan sospechosos.

¿Cómo encaja la Defensa Activa en un programa de seguridad cibernética?

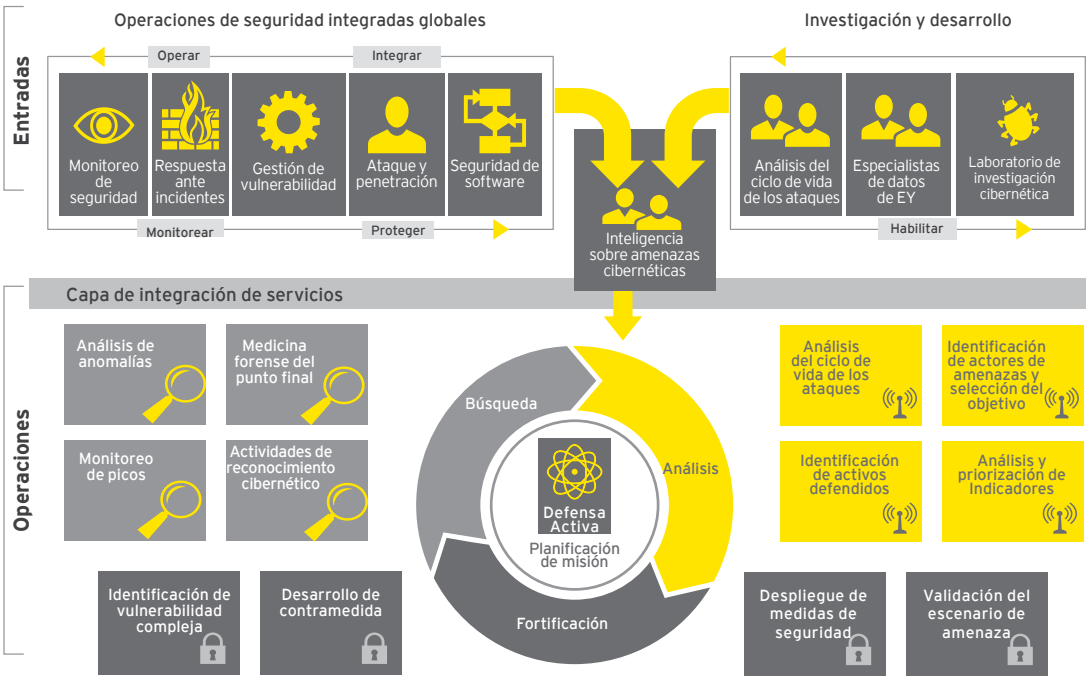
La mayoría de los equipos de operaciones de seguridad carecen de la capacidad de detección, y aquí es donde la Defensa Activa puede realzar la eficiencia organizacional. Empleando un ciclo operativo deliberado para planificar, ejecutar y revisar las actividades dirigidas por inteligencia para ayudar a implementar medidas de seguridad, fortalecer las defensas y buscar a los intrusos, los profesionales de la Defensa Activa proporcionan a la organización la capacidad de identificar y ayudar a erradicar a los atacantes que evaden el monitoreo de seguridad tradicional y apuntan a su propiedad intelectual y sus sistemas empresariales.

Preparar una Defensa Activa

¿Cuáles son los prerrequisitos para establecer un programa de Defensa Activa?

La Defensa Activa es el resultado de la fusión entre el análisis de inteligencia oportuno sobre amenazas con medidas proactivas planificadas y ejecutadas deliberadamente, la cual ayuda a combatir escenarios de amenaza específicos. La Defensa Activa no reemplaza las operaciones de seguridad tradicionales. Más bien, la Defensa Activa organiza y realza el programa de operaciones de seguridad existente. La realización de una Defensa Activa requiere un poco de preparación para lograr una eficacia máxima.

Integración de la Defensa Activa en las operaciones de seguridad



23%

de organizaciones con un COS declararon que este "no interactúa con el negocio".

En primer lugar, los defensores cibernéticos deben asegurarse de tener una comprensión clara de los bienes más codiciados por los atacantes potenciales. En la encuesta Global de Seguridad 2015 de EY, el 23% de las organizaciones con un COS declaró que su este, "no interactúa con el negocio" y sólo el 23% reportó que su SOC "está estrechamente integrado, reuniéndose con los jefes de las operaciones comerciales regularmente para entender las preocupaciones y los riesgos del negocio". Esta interacción es clave y está ausente en muchos programas de seguridad.

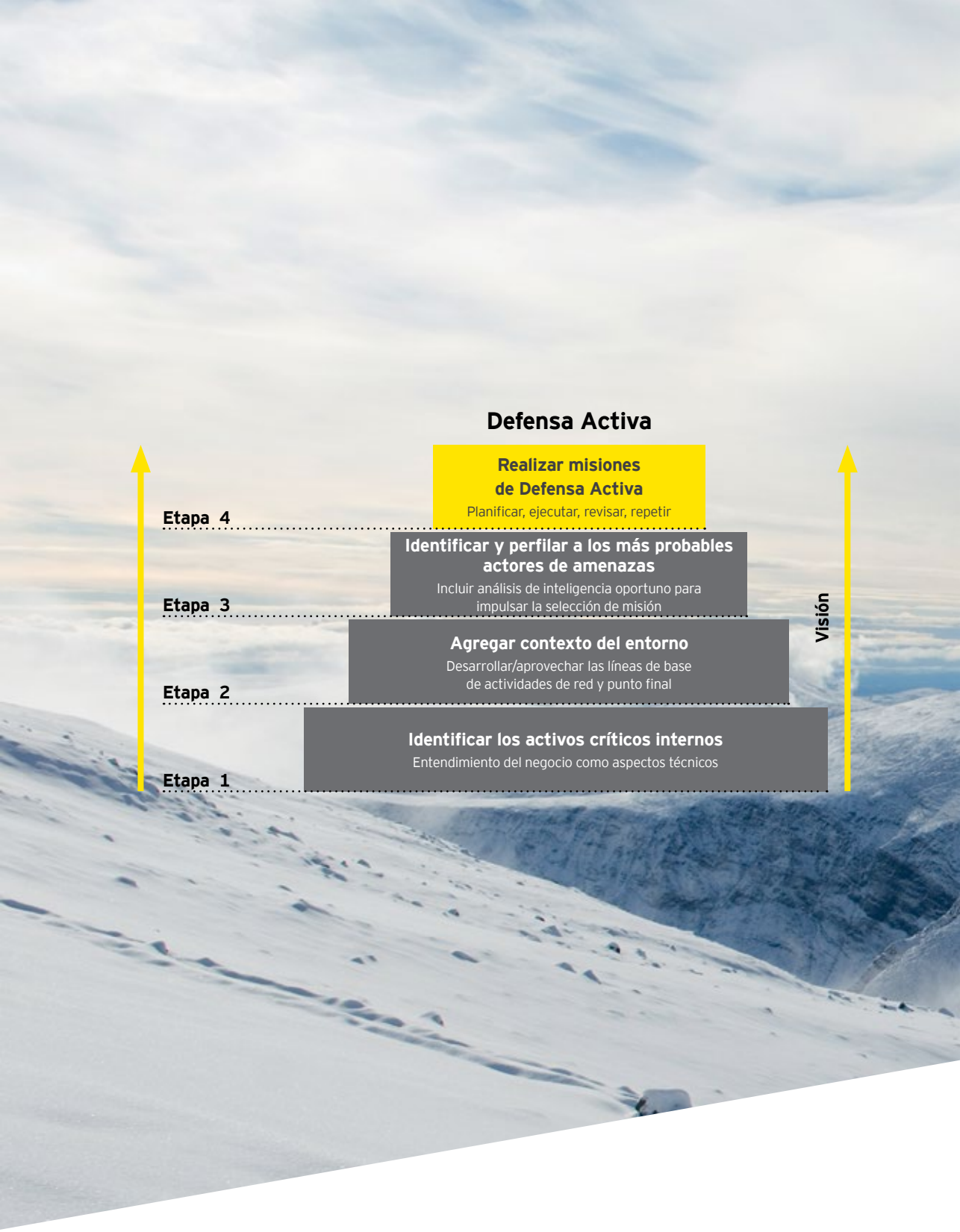
Las conversaciones entre profesionales de seguridad y líderes comerciales producen una lista de activos que deben defenderse. Estos están generalmente asociados con funciones críticas del negocio y se soportan de importantes sistemas, junto con repositorios de datos sensibles. Los activos relevantes serán aquellos que puedan comprometer el negocio a graves consecuencias si son manipulados, robados o dejaran de estar en línea. Los ejemplos incluyen la propiedad intelectual, datos de investigación y desarrollo que sustentan futuras innovaciones, la información personal de los empleados o clientes, información de tarjetas de crédito de los clientes, y los sistemas de control industriales que sustentan las funciones críticas del negocio.

23%

de las organizaciones reportó que, "Nuestro COS está estrechamente integrado, reuniéndose con los jefes de las operaciones del negocio con regularidad para entender las preocupaciones y riesgos de negocio".

¿Qué debo comprender de mi organización para habilitar la Defensa Activa?

Finalmente, los defensores necesitan una comprensión de las amenazas que puedan seleccionar a su organización como objetivo. Muchos equipos de seguridad simplemente asumen que son el objetivo de los tres grandes: naciones-estado adversarias, grupos de crimen organizado y *hacktivistas*. Aunque esto puede ser cierto, se requiere un entendimiento adicional con el fin de elaborar una Defensa Activa. Dentro de cada grupo, las motivaciones y capacidades varían ampliamente. Los defensores deben trabajar en estrecha colaboración con los proveedores de inteligencia sobre amenazas para pintar un retrato exacto del escenario de las amenazas con el mayor detalle posible. Si es posible, los actores específicos de una amenaza deben ser nombrados y analizados para obtener un entendimiento que será aprovechado en las actividades de defensa.


Defensa Activa
Realizar misiones de Defensa Activa
Planificar, ejecutar, revisar, repetir
Etapa 4
Identificar y perfilar a los más probables actores de amenazas
Incluir análisis de inteligencia oportuno para impulsar la selección de misión
Etapa 3
Agregar contexto del entorno
Desarrollar/aprovechar las líneas de base de actividades de red y punto final
Etapa 2
Identificar los activos críticos internos
Entendimiento del negocio como aspectos técnicos
Etapa 1
Visión

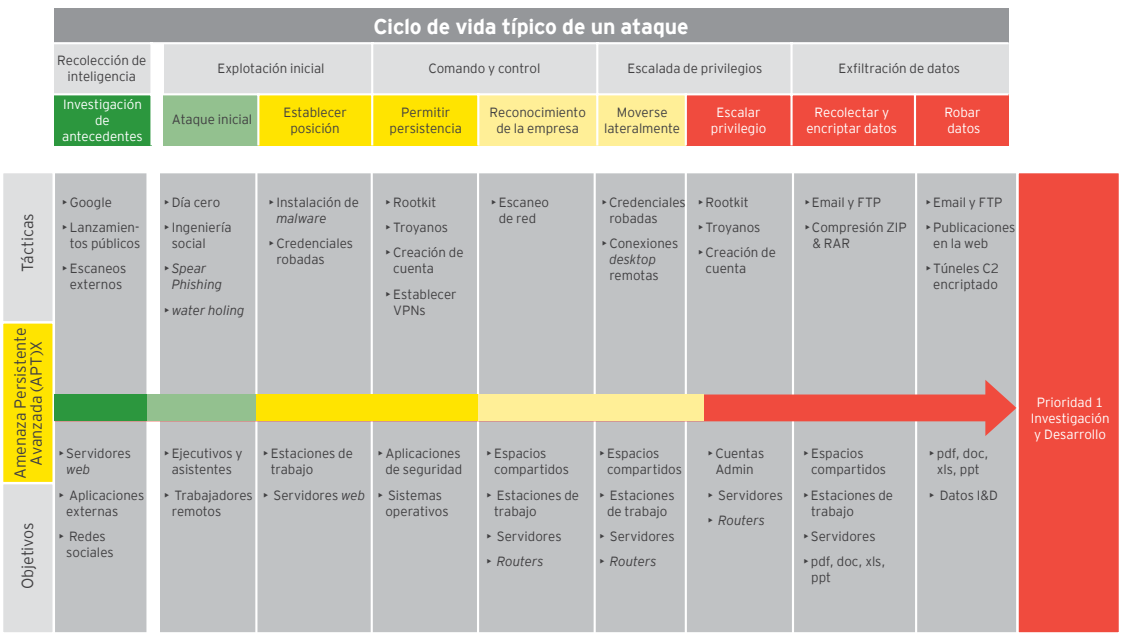
Realiza preparar una Defensa Activa

La Defensa Activa consiste en acciones defensivas planificadas y ejecutadas deliberadamente, llamadas "misiones". Cada misión es seguida por actividades diseñadas para capturar lecciones aprendidas y realzar el aprendizaje organizacional. Las misiones incluyen uno o más objetivos específicos y un estado final definido, y pueden durar entre un día y varias semanas. Los objetivos de la misión incluyen típicamente la implementación de una o más contramedidas dirigidas para derrotar escenarios de amenaza específicos o actividades planificadas deliberadamente para identificar a intrusos ocultos (búsqueda).

Aunque las misiones individuales pueden adoptar la forma de proyectos, un programa de Defensa Activa se lleva a cabo como un ciclo operativo iterativo. Cada ciclo se centra en la defensa de un activo específico o grupo de activos de un actor de amenazas específico y puede incluir una o más misiones. El ciclo operativo incluye las fases de planificación, ejecución de misión (de una o más misiones) y revisión de ciclo. Cada misión dentro del ciclo operativo también incluye fases análogas para la planificación, ejecución y revisión.

¿Cuáles son los componentes de una Defensa Activa?

La Inteligencia sobre Amenazas Cibernéticas (CTI por sus siglas en inglés) ayuda a sentar las bases para la Defensa Activa y proporciona contexto y orientación durante las operaciones. Una vez que se han identificado probables adversarios, los defensores trabajan con su proveedor de inteligencia sobre amenazas para identificar tácticas específicas a través del análisis de la cadena de ataque cibernético. El análisis de la cadena de ataque es la división de los pasos ejecutados por un adversario como parte de un ataque en "fases" individuales que corresponden a los eslabones de la cadena de ataque. Aunque los investigadores de *Lockheed-Martin* originalmente introdujeron este concepto en una nota técnica[3] de 2011, existe una serie de variantes. Independientemente de la variante, la identificación y el análisis de la táctica es clave.



[3] *Hutchins, Eric, Michael Cloppert y Rohan Amin, "Defensa de Red en Computadora Dirigida por Inteligencia Informada por Análisis de Campañas de Adversarios y Cadenas de Ataque de Intrusión" Lockheed Martin Corporation, 2011.*

31%

de los encuestados dice que su COS cuenta con personas dedicadas al análisis de inteligencia de amenazas cibernéticas.

50%

de los encuestados dice que su COS cuenta con analistas que revisan y se suscriben a recursos de fuentes de información gratuita específicas.

Además de las tácticas conocidas, los datos adicionales recopilados y mapeados para reflejar los actores de amenazas relevantes incluyen:

- Rangos IP de la fuente del atacante
- Metadatos de *malware*
- *Hardware* o *software* típicos utilizados por el atacante
- *Hardware* o *software* típicos seleccionados como objetivo por el atacante
- Horas típicas de las operaciones del atacante

Para cada activo defendido, los defensores también recopilan:

- *Hardware* o *software* utilizados para acceder a los datos sensibles y procesos de negocios
- El nivel de parches y cronograma de parches para *hardware* y *software* identificados
- Información de ataques anteriores
- Identidad detallada e información de acceso asociada con el recurso

Esta información se suplementa con inteligencia sobre eventos actuales en la industria de la organización para determinar quién está atacando a sus pares y con qué propósito. Los pares de la industria son una gran fuente para desarrollar un entendimiento de primera mano sobre las últimas herramientas, tácticas y procedimientos utilizados por los atacantes.

35% de los encuestados dice que tienen una estrategia de seguridad de la información madura o muy madura.

Sólo el **12%** de las organizaciones realizan todas las funciones de operaciones de seguridad internamente.

23% de los COS no interactúan con el negocio.

29% de los COS colaboran y comparten datos con otros COS públicos.

43% de los COS colaboran y comparten datos con otros en su industria.

42% de los COS no han detectado un incidente importante.

Sólo el **19%** de los COS han descubierto un incidente de seguridad cibernética significativa.

Sólo el **47%** de las organizaciones piensan que su COS podría probablemente detectar un atacante sofisticado.

¿Qué es una misión de Defensa Activa?

Un aspecto clave de la Defensa Activa es el enfoque y la eficacia operativa realizada a través de la planificación deliberada de las misiones. Los equipos de seguridad típicamente refuerzan sus defensas sobre una base ad hoc, implementando las mejores prácticas de la industria cuando tienen tiempo o en reacción a anuncios de vulnerabilidad de gran visibilidad. Por contraste, las misiones de Defensa Activa se planifican y ejecutan de forma proactiva para vencer escenarios de amenaza específicos y descubrir intrusos ocultos en la red. Esto significa que los defensores pasan su tiempo disuadiendo y derrotando a los atacantes más probables de la empresa, y no a un adversario no definido o no específico.

¿Qué tipos de misiones puedo realizar con la Defensa Activa?

El uso del término "misión" expresa el hecho de que el proceso operativo procede con una cantidad significativa de rigor analítico y disciplina con el fin de lograr la máxima eficacia en el cumplimiento de los objetivos de seguridad de la organización. Las misiones son planificadas en respuesta a la inteligencia de amenazas específicas en el contexto singular de la organización defendida; y centrándose en la amenaza al negocio a partir de los escenarios de amenaza en el mundo real, los profesionales de Defensa Activa pueden maximizar sus capacidades de defensa a su presupuesto de seguridad.

Aunque la Defensa Activa se centra inherentemente en el adversario, también se adapta a activos defendidos específicos — típicamente, los datos propietarios y sistemas de negocio más valiosos de la organización. Una misión de Defensa Activa puede incluir cualquier actividad que cumpla esta descripción. Pero, encontramos que algunas categorías generales de actividades tienden a generar los mayores retornos de inversión.

Categorías de misiones de Defensa Activa

Protección	Búsqueda
Reconocimiento de la red Identificación y validación manual de vulnerabilidades complejas y escenarios de amenazas y el desarrollo del conocimiento situacional de la red para los decisores.	**Análisis de anomalías** Investigación enfocada en detectar actividades anómalas y maliciosas que no pueden ser detectadas con herramientas automatizadas de monitoreo de seguridad.
Contramedidas dirigidas Aprovechar entendimientos a partir del proceso de inteligencia para diseñar e implementar contramedidas que derrotan escenarios de amenazas específicas.	**Captura y coacción** Alterar las condiciones de la red y de punto final para provocar a un atacante oculto a que realice actividades maliciosas susceptibles de ser detectadas por un monitoreo dirigido intensivo.

41%

de los encuestados dice que su COS tiene una suscripción pagada a fuentes de información de inteligencia sobre amenazas.

Protección

La primera categoría de la misión de Defensa Activa incluye aquellas actividades que ayudan a mejorar las defensas de la empresa contra las tácticas específicas que pueden ser utilizadas por atacantes específicos.

Reconocimiento de la red

Las misiones de reconocimiento de la red desarrollan la comprensión de la organización acerca de su propio nivel de riesgo de vulnerabilidad ante actores o escenarios de amenazas específicas. Las misiones de este tipo son generalmente más complejas que el escaneo sencillo de vulnerabilidades y pueden incluir simulacros de ataque o ejercicios del equipo rojo. Un ejemplo de una misión de recopilación de información sería un experimento de varios días para determinar si las herramientas de monitoreo de seguridad existentes son capaces de identificar el uso de una determinada pieza de *malware* en la red.

Medidas de seguridad personalizadas

Las medidas de seguridad personalizadas más a menudo se centran en la fortificación de la red y el punto final e intentan disuadir, degradar o derrotar las tácticas específicas del adversario. Las actividades de fortificación de Defensa Activa difieren de las actividades de refuerzo ejecutadas por los equipos de operaciones de seguridad tradicionales en que se ejecutan deliberadamente en respuesta a la inteligencia de amenazas oportuna sobre un actor de amenazas o escenario de amenaza, y no como "las mejores prácticas de la industria" sobre una base ad hoc.

- "Limpiar y mantener" es un ejemplo de protección de la red

  Un tipo de protección de la red, es la de "limpiar y mantener" la cual es una estrategia empleada para ayudar a evitar que intrusos vuelvan a ocupar el territorio del cual han sido expulsados por los defensores. La limpieza se realiza a través de la búsqueda o análisis forense proactivo. Después de la etapa de limpieza, la fase de mantenimiento se caracteriza generalmente por inspecciones regulares, vigilancia y mejora de las defensas.

  Una misión del tipo "limpiar y mantener" puede estar garantizada por una serie de factores internos o externos. Los defensores pueden enterarse de un ataque contra un par de la industria y pueden desear aplicar tácticas de "limpiar y mantener" para proteger los tipos de datos que fueron tomados en ese ataque. Otra motivación podría ser el descubrimiento de una vulnerabilidad que no puede ser parchada en un sistema crítico. Los *hosts* en el mismo segmento de red podrían ser limpiados para asegurarse de que no estén albergando actualmente atacantes que podrían aprovecharse de la debilidad.

  Las actividades de esta naturaleza sólo pueden mantenerse por un breve período de tiempo antes de que los recursos deban ser desplegados hacia otras áreas. Por ejemplo, una misión de "limpiar y mantener" probablemente sería apropiada durante el período en que se está planeando una fusión/adquisición (desde las primeras etapas) y ejecutada. Una vez que la fusión se anuncie públicamente y se complete, la protección proporcionada por las tácticas de "limpiar y mantener" ya no es necesaria en torno a los sistemas que contienen datos de fusión.

47%

de encuestados reportó que su organización no tiene actualmente un COS.

Búsqueda

Las misiones de búsqueda intentan descubrir atacantes latentes (pero activos) en la red, o la evidencia previamente desconocida de ataques anteriores. Al examinar activamente actividades o artefactos aparentemente benignos en el contexto de tácticas y técnicas conocidas de determinados actores de amenazas o en el contexto de escenarios de amenazas específicas, los profesionales de Defensa Activa toman la iniciativa contra los atacantes y reducen el tiempo que los atacantes pueden esperar tener para operar dentro de la red antes de ser identificados y erradicados. Las misiones de búsqueda caen generalmente en dos categorías.

26%

de los encuestados que sí tiene un COS, el 26% subcontrata el monitoreo de seguridad en tiempo real.

Análisis de anomalías

Estas misiones examinan artefactos ubicados en *hosts* particulares junto con patrones de tráfico de red para identificar actividades maliciosas que las herramientas automatizadas de monitoreo de seguridad no perciben. Aunque la organización puede tener un despliegue sofisticado e integral de sensores para llevar a cabo el monitoreo de seguridad para los segmentos y los puntos finales de la red, hay muchas formas de actividad maliciosa que impiden la detección automática, pero que son simplemente obvias para los analistas humanos.

Como hemos comentado anteriormente, la capacidad de identificar actividades anómalas es uno de los habilitadores clave de la Defensa Activa y es crítica para las misiones de búsqueda. La actividad anómala es cualquier actividad que sea extraña, anormal o que no pertenezca al contexto en el que se ve. Este contexto podría incluir al usuario que está realizando la actividad, la hora en el que se observa la actividad, la frecuencia con que se produce la actividad y otras circunstancias. Además de buscar la actividad anómala en nuevos flujos de eventos, los defensores deben asegurarse de buscar datos históricos también.

El momento en que los defensores se dan cuenta de un comportamiento malicioso en particular es usualmente después del momento en que los atacantes comenzaron a usar dicha información: por lo tanto, se debe inspeccionar los registros históricos para asegurarse que no se haya producido ya un compromiso de la data.

- Identificar las bases de operaciones cibernéticas

  El análisis de anomalías puede ser utilizado para identificar las bases de operaciones cibernéticas, y para disuadir o impedir la filtración de datos sensibles. Los atacantes a menudo toman una "cabeza de playa" dentro de una red comprometida. Se trata de un *host* desde el cual ellos lanzan incursiones contra otros *hosts* de la red y en el cual ellos pueden almacenar datos robados. A menudo estos datos son comprimidos, disfrazados, o incluso encriptados, para que se vean como algo que no son. Por ejemplo, los defensores pueden descubrir un gran escondite de datos insertados en varios archivos RAR encriptados y comprimidos, cuyas extensiones de archivo han sido alteradas para que se vean como videoclips.

  Este concepto de "cabeza de playa" es importante porque los *hackers* deben preparar una base de operaciones a uno o dos "saltos" de un lugar en la red desde el cual serán robados los datos. No solo se requiere esto para limitar la cantidad de actividad en un *host* objetivo a fin de evitar ser detectados, sino que el enrutamiento de conexiones y datos a través de sistemas adicionales es técnicamente complicado y difícil de detectar en sí.

  Para identificar las bases de operación, los defensores buscan probables ubicaciones de "cabeza de playa" cerca de los sistemas sensibles, destinados a datos robados y herramientas almacenadas. En las empresas que establecen ubicaciones de almacenamiento de datos para los usuarios, esta búsqueda puede ser sencilla. La búsqueda también puede facilitarse con el uso de nomenclatura de archivos de la empresa. Estos a menudo no son evidentes para personas ajenas, por lo que los atacantes pueden crear inadvertidamente nombres de archivos que inmediatamente se revelan como anómalos.

Captura y coacción

Estas misiones intentan empujar a los atacantes latentes a llevar a cabo actividades que harán que sean descubiertos. Una vez que un atacante obtiene acceso a la red con privilegios sensibles de manera permanente, es improbable que realicen actividades maliciosas públicas adicionales. Esto se debe a que probablemente hayan obtenido acceso a credenciales de cuentas legítimas o hayan tenido la oportunidad de instalar un *software* malicioso para enmascarar,

12%

de encuestados que sí tiene un COS reportaron que pueden cumplir con todas las funciones internamente.

limpiar u ocultar sus actividades. Al alterar las condiciones en la red, los defensores pueden imponer un dilema a los atacantes ocultos. Ellos deben trabajar para mantener su acceso y someterse al escrutinio de los profesionales atentos de Defensa Activa, o perderán el acceso. Estos son ejemplos de este tipo de misión:

- Acabar con el *malware*

  Muchos tipos de *malware* emiten una "prueba ping" o "latido de corazón" regular a un servidor de comando y control (C&C) mientras están activos. Esto tiene dos propósitos. En primer lugar, actúa como una notificación remota para un atacante que le dice que su acceso a la red sigue disponible. En segundo lugar, proporciona a los sistemas de control automatizados la oportunidad de emitir órdenes a las instancias del *malware* colocados en el terreno (implantes).

  Los atacantes altamente sofisticados pueden emplear múltiples formas de *malware* cooperativo que se miran entre sí para proporcionarse respaldo. Si un implante ve que su asociado ha sido erradicado o ya no se comunica en la red, se activa y se hace cargo de emitir los "ping" y ejecutar la actividad maliciosa. En nuestra experiencia hemos visto redes que tenía implantes primarios instalados en más de 20 servidores, con implantes alternativos o de copia de seguridad ocultos en otros 14. Los alternativos no fueron detectados hasta que los primarios fueron erradicados — el punto en que un equipo de respuesta a incidentes por lo general cerraría el caso y se iría a casa.

  Los cambios en la conectividad de la red son usualmente la causa que da lugar a la activación de los implantes latentes. Considere simular esto para "acabar con" el *malware* de su acceso a la red y cambiar su comportamiento. Los segmentos de la red se pueden cortar entre sí temporalmente para evitar que las muestras

cooperativas del *malware* se vean entre sí o interactúen unas con otras; esto puede ocasionar una espiral de multiplicación del *malware* que trata de tomar el lugar de lo que piensa que es un primario erradicado.

- Manipulación del DNS

  Los autores de los *malware* utilizan típicamente nombres de *hosts* para configurar los servidores C&C del *malware* en lugar de direcciones IP. Esto mejora la resiliencia para el *malware*, ya que los defensores típicamente bloquean el tráfico de salida a direcciones IP específicas (los *routers* y los *switches* no saben acerca de nombres de *host*). El uso de un nombre de *host* permite al servidor de C&C del *malware* ubicarse en cualquier dirección IP. El atacante sólo tiene que registrarlo y los servidores DNS de todo el mundo le llevarán la noticia a su *malware* desplegado. Los defensores que han tratado de aplastar una infección de *malware* probablemente han visto este comportamiento antes: ellos bloquean el tráfico saliente para el *malware* que envía a los "pings", sólo para verlo cambiar a nuevas direcciones de destino cada pocas horas.

  Al reiniciar el caché del DNS de la red, los defensores obligan a la renovación de cada nombre de *host* a través de la red — incluyendo aquellos utilizados por el *malware*. Pocas horas o días después, los defensores pueden entonces examinar el contenido del caché DNS para identificar nombres de *host* de baja densidad o nombres de *host* que fueron resueltos en horas extrañas. Una gran cantidad de conexiones a www.google.com al mediodía de un martes no debería levantar sospechas, pero una sola conexión a www.malwaremothership.com a las 2 a.m. de un martes amerita una inspección más de cerca.

¿La Defensa Activa es adecuada para mi organización?

EY considera la posibilidad de montar una Defensa Activa eficaz como un estado final estratégico para un programa de seguridad de la empresa, y el trayecto para establecer una Defensa Activa eficaz varía para cada organización. De acuerdo con nuestra Encuesta Global de Seguridad 2015, el 47% de los encuestados reportó que su organización no tiene actualmente un COS; de aquellos que sí lo tienen, el 26% subcontrató el monitoreo de seguridad en tiempo real, y sólo el 12% reportó que pueden cumplir con todas las funciones internamente.

¿Mi organización está lista para implementar una Defensa Activa?

Las ofertas de seguridad cibernética de EY ayudan a desarrollar el programa de seguridad con miras a establecer una Defensa Activa. Sin embargo, si alguna de las siguientes afirmaciones refleja su organización, entonces la Defensa Activa puede ser la solución apropiada para su organización:

- ☐ Tenemos un COS, pero seguimos sin encontrar pruebas de atacantes avanzados.
- ☐ Tenemos un COS, pero a pesar de ello tuvimos una violación importante.
- ☐ Hemos tenido un COS durante unos años, pero tenemos que evolucionar más allá del monitoreo estático.
- ☐ Tenemos fuertes presiones empresariales para defender la propiedad intelectual o información confidencial de la empresa (R&D, M&A, ICS/SCADA, etc.).
- ☐ Tenemos un COS subcontratado, pero no creemos que nuestros datos y sistemas más valiosos estén realmente protegidos.

47%

de los encuestados reportó que su organización no tiene actualmente un COS.

¿Cómo puede ayudarme EY a prepararme para realizar una Defensa Activa en el futuro?

Muchas organizaciones pueden beneficiarse de la disciplina operativa realizada y del enfoque en el adversario, inherentes a la Defensa Activa. Sin embargo, la eficacia de un programa de Defensa Activa requiere niveles de madurez apropiados en una gama de competencias de seguridad, incluyendo las operaciones de seguridad, el monitoreo de seguridad, la identificación y clasificación de activos, las operaciones informáticas, la inteligencia sobre amenazas, la arquitectura de seguridad y otros. Al centrarse en una capacidad de Defensa Activa como un objetivo estratégico, los decisores y los profesionales de la seguridad pueden entablar una conversación significativa acerca de los pasos necesarios para la mejora organizativa que ayudará a realizar los beneficios que se describen en el presente documento.

Cuando esto ocurre, los beneficios de una Defensa Activa pueden ser:

Para el equipo de operaciones de seguridad, la Defensa Activa ayuda a proporcionar un conjunto definido de actividades de mejora racionalizadas por la inteligencia sobre amenazas y la analítica de seguridad; y luego conectado a objetivos alcanzables. El equipo construye medidas de seguridad, busca intrusos ocultos y refuerza las defensas sobre la base de informes reales sobre la conducta de atacantes reales.

Para los decisores, la Defensa Activa ayuda a conectar el despliegue de recursos directamente a las medidas de la eficacia del programa de seguridad cibernética. En lugar de centrarse en medidas de desempeño como el "número de parches aplicados" y el "número de tickets cerrados", la eficacia puede demostrarse, por ejemplo, a través de una disminución de los ataques dirigidos exitosos o de una disminución del tiempo requerido para descubrir y erradicar los ataques que fueron exitosos.

La propiedad intelectual y los sistemas críticos del negocio de una organización tienen un importante valor monetario, y los líderes de las organizaciones esperan que sus programas de seguridad conserven los datos seguros y los atacantes afuera. Con este fin, la eficacia de las operaciones de seguridad de la organización puede ser realzada de manera significativa por una Defensa Activa guiada por una planificación, un estado final estratégico definido y un enfoque en el adversario. Mediante la organización y la integración de las operaciones de seguridad existentes de la organización, la Defensa Activa puede ayudar a reducir el número de ataques dirigidos exitosos y disminuir la cantidad de tiempo en que los intrusos pueden operar antes de ser expulsados de la red.

¿Cuáles son los beneficios de una Defensa Activa?

- Un ciclo operativo ágil diseñado para ayudar a lograr resultados rápidos y acelerar el aprendizaje.
- El análisis de Inteligencia sobre Amenazas Cibernéticas (CTI) que ayuda a a entender mejor a los atacantes y elaborar recomendaciones.
- Las misiones de Defensa Activa centradas en la búsqueda o la protección.
- La Defensa Activa ayuda a realzar, pero no reemplaza el monitoreo de seguridad y la respuesta ante incidentes tradicionales.

Anexo 02

Usando *Analytics* para adelantarnos al crimen cibernético.
Los Centros de Operaciones de Seguridad de Tercera Generación.

¿El uso de *Analytics* puede ayudar a prevenir el crimen cibernético?

En un mundo cada vez más conectado, proteger los activos digitales de una organización es una preocupación empresarial clave. La seguridad cibernética ya no es considerada como un tema técnico sino que es reconocida como un desafío empresarial fundamental para la mayoría de las organizaciones.

A medida que las diversas amenazas siguen evolucionando rápidamente, tanto en sofisticación como en escala, la necesidad de proteger la propiedad intelectual, las operaciones, la marca y los intereses de la organización, y en adición, la información de sus clientes, es cada vez más crítica. Los avances en la industria de seguridad no se han ajustado al ritmo del conjunto diverso de amenazas de hoy en día; por lo tanto, las organizaciones se encuentran en una posición en la que los productos vigentes y los servicios tradicionales no son suficientes para enfrentar el riesgo.

Existe la necesidad de estrategias más audaces y de innovación en la seguridad cibernética. Si prepararse para ataques conocidos, es bastante difícil. ¿Cómo pueden las organizaciones controlar los riesgos de seguridad que aún no conocen?.

Las organizaciones líderes están haciendo más que mejorar su estado actual, están buscando incrementar sus esfuerzos – para tomar medidas más audaces – para combatir las amenazas cibernéticas y ajustarse al ritmo de los atacantes cibernéticos, o incluso tomarles la delantera.

En lugar de esperar que las amenazas se presenten, estas organizaciones están aprovechando en analizar las amenazas para priorizar los esfuerzos que permitan poseer una mayor visibilidad y una Defensa Activa a través de la supervisión personalizada, el análisis, la búsqueda y la rápida detección sobre la información y sistemas de mayor importancia.

En años recientes, las organizaciones han reconocido los beneficios de tener un adecuado Centro de Operaciones de Seguridad (COS).

12%

de las organizaciones considera bastante probable que puedan detectar un ataque sofisticado.

46%

de las organizaciones no cuenta con un COS.

Estos incluyen, el permitir que las funciones de seguridad cibernética respondan oportunamente, trabajen de manera más colaborativa y compartan conocimientos de manera más efectiva. Los COS de primera generación tendían a enfocarse en los controles basados en firmas, tales como los sistemas antivirus y de detección de intrusión, permitiendo que las organizaciones detecten los factores asociados con un ataque. La segunda generación de COS auguró la llegada de las operaciones 24x7, reconociendo que los atacantes no culminan su día laboral, a pesar que las empresas sí lo hagan.

Hoy en día estamos observando el surgimiento de la tercera generación de Centros de Operaciones de Seguridad en base al desarrollo de un análisis de inteligencia sobre las amenazas y la cibernética para permitir una Defensa Activa. Las organizaciones líderes buscan aprovechar las plataformas de análisis cibernético construidas sobre una arquitectura de procesamiento de datos de gran volumen.

Esta arquitectura combina el procesamiento por lotes y el procesamiento en tiempo real, el cual permite poder contar con capacidades de detección de anomalías en base a análisis matemáticos y al modelamiento estadístico que puede manejar *terabytes* de datos diariamente. La tercera generación de COS también facilita la búsqueda proactiva de violaciones de seguridad, la integración de un marco de gestión de amenazas cibernéticas en la empresa y la convergencia entre la ciencia del análisis de datos y las operaciones de seguridad, permitiendo a las organizaciones procesar grandes volúmenes de datos para poder contar con indicadores oportunos de seguridad.

Una ventaja clave que resulta de la implementación de una plataforma de análisis cibernéticos, es su agilidad en el uso del análisis de datos para acelerar la capacidad de detección y respuesta ante incidentes de seguridad. Esto incluye mecanismos para controlar posibles ataques a través de modelos personalizados de prevención.

¿Por qué los Centros de Operaciones de Seguridad han cambiado?

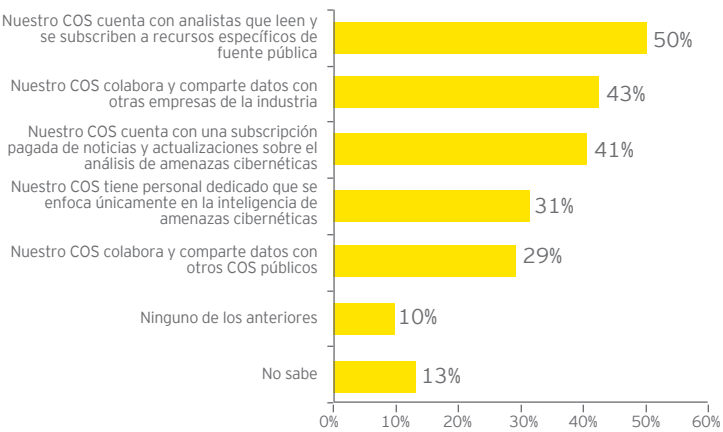
¿Qué hace un COS?

Un Centro de Operaciones de Seguridad con buen funcionamiento puede ser el corazón de la detección efectiva. Puede permitir que las funciones de seguridad de una la información respondan de forma oportuna, trabajen de manera más colaborativa y compartan conocimiento de manera más eficiente.

El propósito de este documento es proporcionar al lector entendimientos sobre la evolución de los COS en el contexto de las amenazas cibernéticas emergentes. Para una vista general más profundizada de los principios fundamentales de los COS, recomendamos leer Centros de Operaciones de Seguridad – ayudándole a tomar la delantera sobre el crimen cibernético.

www.ey.com/SOC

¿Cómo los COSs siguen el ritmo de las amenazas más recientes?



En comparación con los resultados de la encuesta del año anterior, los encuestados del 2015 registraron un incremento marcado en los aspectos de cómo sus COS se mantienen al día acerca de las más recientes amenazas. Esto indica que las organizaciones están realizando mayores esfuerzos concertados para formalizar y expandir las capacidades de sus COS para afrontar mejor las amenazas emergentes y cada vez más sofisticadas.

51%

de las organizaciones con un COS inician una investigación a menos de una hora del descubrimiento de un incidente.

23%

considera que su COS está estrechamente integrado con los gerentes de las empresas para comprender con regularidad las preocupaciones del negocio.

42%

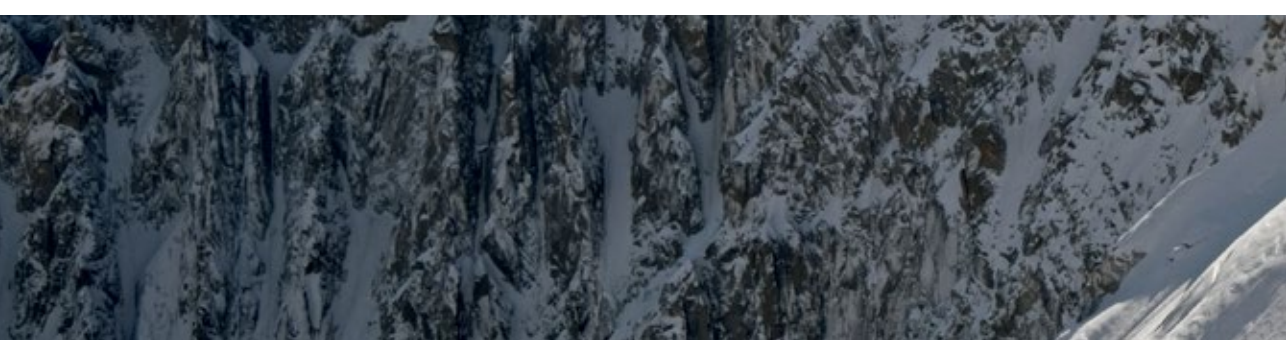
de las organizaciones afirma no haber tenido un incidente significativo.

Principios del COS de tercera generación

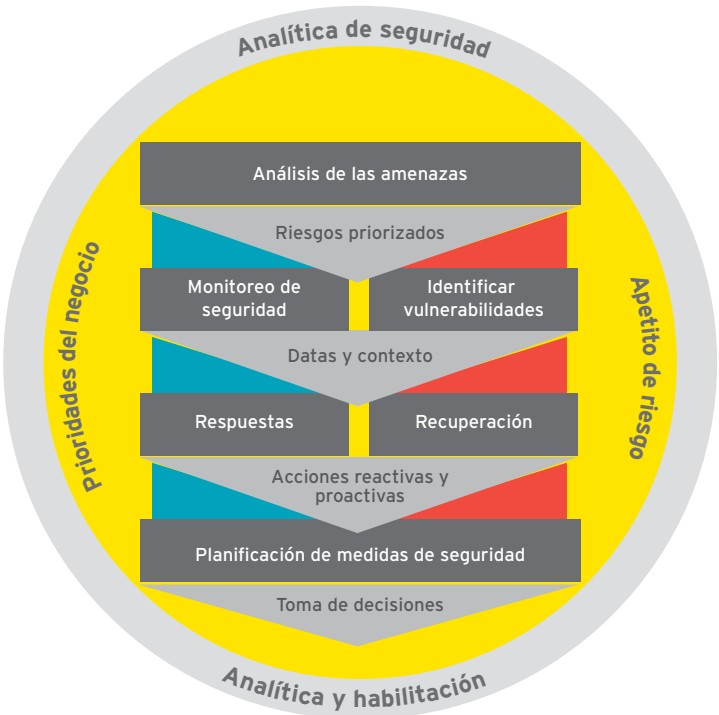
Si bien, detectar actividades inusuales continúa siendo una función relevante de un COS, los COS de tercera generación han evolucionado para enfocarse en identificar nuevas amenazas, para las cuales no se ha observado ninguna línea base anteriormente. Para obtener esta capacidad, las organizaciones necesitan integrar y alinear sus distintos recursos e inversiones de seguridad cibernética, tal como se establece en los siguientes principios rectores:

- **Operaciones de Seguridad Integrada**
  Mientras que las organizaciones continúan aumentando significativamente sus inversiones en seguridad cibernética, las amenazas continúan acelerándose y superando las defensas de seguridad tradicionales y los enfoques operativos. Esto hace que muchas organizaciones se preocupen por identificar dónde enfocar su inversión y sus iniciativas de mejora. Asimismo, la necesidad de establecer un contexto más sólido que apoye a la toma de decisiones de seguridad cibernética operativa y estratégica, es clave. La tercera generación de operaciones de seguridad requiere un enfoque que contemple a toda la empresa, y que integre las distintas inversiones y actividades de seguridad cibernética de la organización.

- **Marco de Gestión de Amenazas Cibernéticas en la Empresa**
  Un COS de tercera generación requiere que se diseñe un marco de gestión de amenazas cibernéticas en la empresa y que se integre completamente de acuerdo a las necesidades clave del negocio. El beneficio de contar con un adecuado marco de gestión de amenazas cibernéticas, permite que una organización alinee sus objetivos de seguridad cibernética con la diversidad de amenazas que se van presentando, así como con las prioridades de la organización y su apetito de riesgo. Dichos marcos también permiten a las organizaciones maximizar las inversiones en seguridad cibernética que pueden haber sido realizadas en la organización.



Marco de Gestión de Amenazas Cibernéticas de la Empresa



Modelo de funcionamiento de las operaciones de seguridad de tercera generación

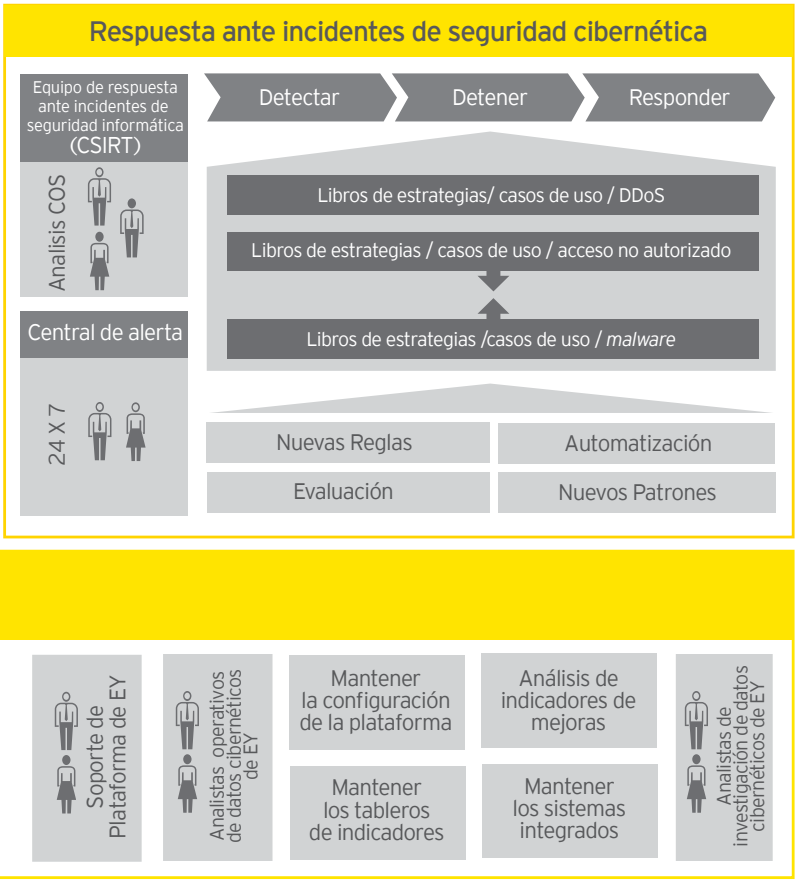
Los principios del COS de tercera generación otorgan el poder a una organización para implementar un modelo operativo que respalde el marco de gestión de las amenazas cibernéticas e integre de manera transparente todas las disciplinas de seguridad cibernética, incluyendo: gestión de amenazas, análisis de inteligencia sobre amenazas, gestión de vulnerabilidades y el análisis cibernético.

Además, estos principios ayudan a una organización a definir un conjunto de mejoras de manera clara, que se encuentran relacionadas con objetivos realizables. El equipo establece medidas de seguridad, búsqueda de intrusos y fortalece las defensas en base a informes sobre la conducta de atacantes reales.

Esto permite a la alta dirección poder alinear los recursos necesarios a las medidas establecidas por el programa de seguridad cibernético.

Para mayor orientación sobre la construcción de un programa de seguridad cibernético efectivo, sírvase remitirse a Gestión de Programa Cibernético – Informe sobre la identificación de las formas de tomar la delantera al crimen cibernético.

www.ey.com/CPM




TRADITION

¿Cómo puede ser impulsada la Defensa Activa por las amenazas?

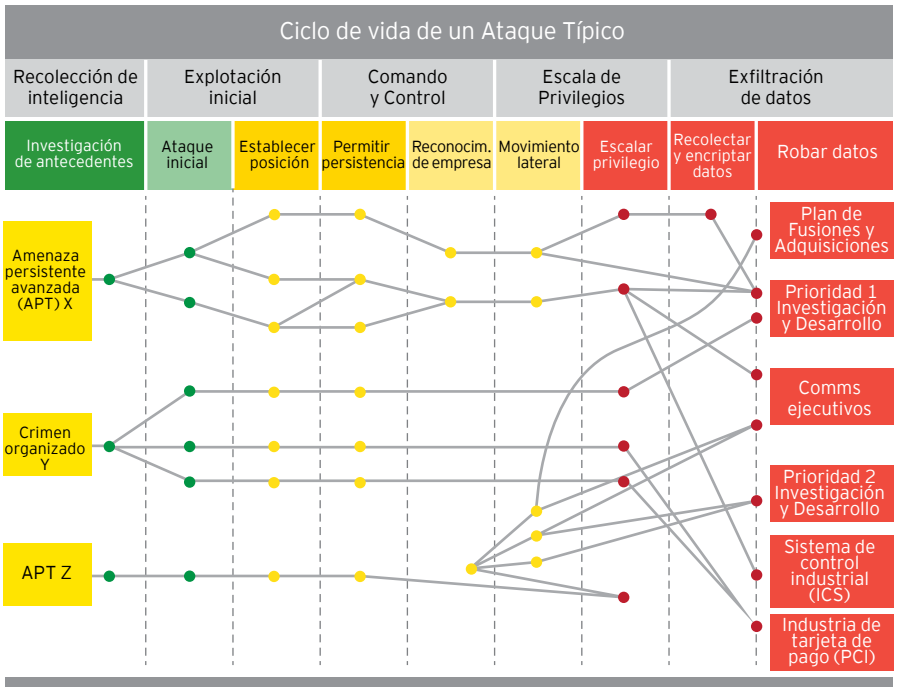
La defensa activa es un conjunto de medidas planificadas que se ejecutan de forma continua para identificar y erradicar a los atacantes y así lograr salir victorioso de probables escenarios de amenazas que apunten a los activos críticos de una organización.

La defensa activa es un ciclo ágil, diseñado para lograr rápidos resultados y acelerar el proceso de aprendizaje. El análisis de inteligencia sobre Amenazas Cibernéticas permite conocer mejor a los adversarios o la empresa y generar así recomendaciones aplicables que permitan al Equipo de Defensa Activa ejecutar acciones enfocadas en el fortalecimiento de su entorno tecnológico. Es importante considerar que la Defensa Activa acentúa pero no reemplaza el seguimiento que realiza el área de seguridad y la respuesta ante incidentes.

Ajustarse al ritmo de determinados atacantes requiere una investigación constante y capacidad de traducir una estrategia empresarial en un análisis de inteligencia aplicable, comprendiendo aquello que hace exitoso al negocio y así poder aplicar la óptica cibernética para comprender:

- ¿**Quién** querría atacar la organización (por ejemplo, estado-nación, activistas o criminales cibernéticos)?
- ¿**Qué** buscarían los adversarios? Las organizaciones deben comprender cuáles son sus activos empresariales críticos.
- ¿**Cómo** intentarían los adversarios atacar a la organización? Esto incluye comprender qué tipos de técnicas usarían (por ejemplo, campañas de *phishing*, ingeniería social, etc.).

Las organizaciones deben supervisar los objetivos estratégicos, medidas técnicas y motivos que motivarían a sus adversarios.



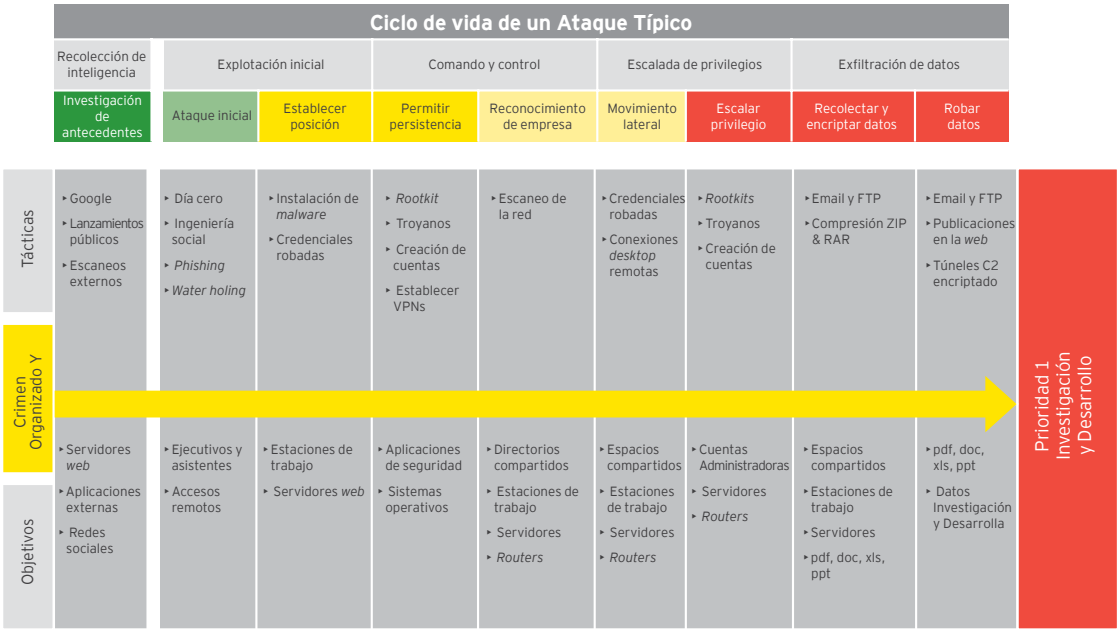
- Los COSs con mayor madurez poseen una conciencia funcional incorporada de los activos de gran valor provenientes de su organización y de las amenazas externas.
- Estos integran el análisis de inteligencia sobre amenazas, supervisión de seguridad, respuesta ante incidentes y gestión de vulnerabilidades de la red y de aplicación, para comprender las posibles vías de ataque avanzadas y desplegar contramedidas.
- Al suministrar al COS de información aplicable sobre amenazas, la organización identifica las vías, tácticas, técnicas y procedimientos con mayor probabilidad de ser usados por los atacantes hacia sus activos críticos.

Paso 1: Identificar activos de alto valor e información crítica.

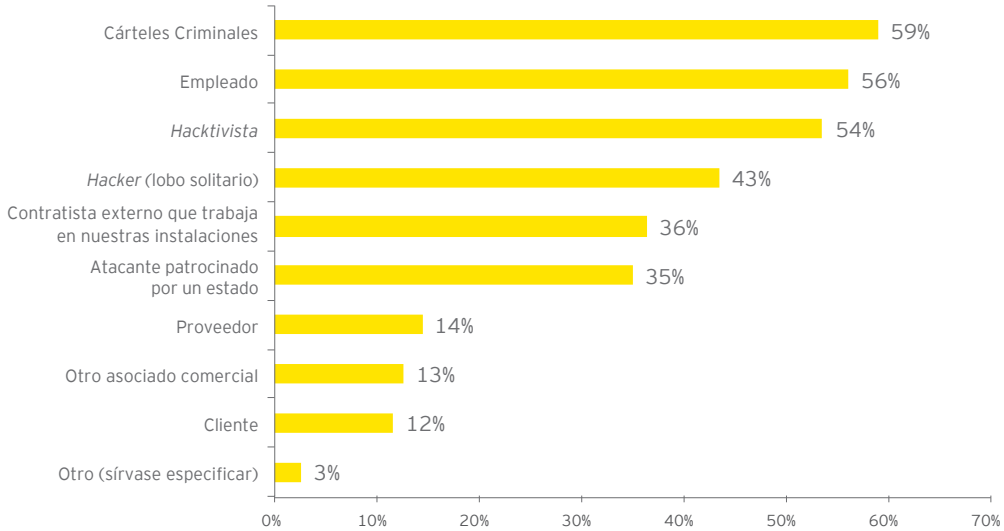
Paso 2: Identificar posibles atacantes (análisis de inteligencia/ incidentes previos).

Paso 3: Identificar las posibles acciones que se realizarán por parte de atacantes potenciales.

Paso 4: Utilizar la información sobre amenazas para identificar las tácticas y objetivos de mayor uso por parte de atacantes.



¿A quién o a qué considera usted como la fuente más probable de un ataque?



Las respuestas sobre las fuentes más probables de un ataque han permanecido relativamente estáticas entre 2014 y 2015. La excepción clave está relacionada con actores externos más organizados (y a menudo más sofisticados), tales como cárteles criminales, atacantes financiados por un estado y hacktivistas. El aumento de la preocupación sobre los atacantes externos especializados es consistente en un año en el cual se han dado distintos ataques de amenaza persistente avanzada (APT) y de muy alto perfil. Las organizaciones están cada vez más conscientes de la necesidad de enfrentar la amenaza generada por adversarios especializados.

60%

dice que el manejo de incidentes graves y su evaluación son presentados regularmente al Directorio de la organización.

Una vez que las organizaciones comprenden las necesidades del negocio, el riesgo, y el análisis de inteligencia sobre amenazas específicas de la industria, la supervisión de seguridad especializada en amenazas y la gestión de vulnerabilidades, se necesita relacionar todo ello con la cadena de ataque. Esto proporciona la facultad de ver qué tipos de técnicas de ataque son utilizadas y el tipo de activos que el atacante tendría como objetivo. Con una cadena de ataque bien identificada, las organizaciones estarán mejor posicionadas para ejecutar la planificación de contramedidas, la búsqueda, el análisis de anomalías y demás.

La Defensa Activa no reemplaza el campo de acción del área de operaciones de seguridad tradicional. Sin embargo, la efectividad máxima de un programa de Defensa Activa requiere niveles de madurez apropiados considerando un rango de competencias. Dicho rango incluye competencias de operaciones de seguridad, tales como seguimiento e inteligencia sobre amenazas, además de actividades tales como identificación y clasificación de activos. Enfocándose en la capacidad de Defensa Activa como nivel de madurez deseado, los decisores y profesionales de la seguridad pueden discutir sobre los pasos necesarios para la mejora organizacional. Las actividades incluyen:

33%

de las organizaciones no cuenta con un programa de análisis de inteligencia sobre amenazas.

1. Protección

a. Medidas personalizadas: Utilizar el entendimiento del proceso para diseñar e implementar las contramedidas que sirvan para salir victorioso en escenarios con amenazas específicas.

b. Reconocimiento de red: Identificación manual y validación de las vulnerabilidades complejas y de escenarios de amenazas; así como el desarrollo de una red de conciencia para los decisores.

2. Búsqueda

a. Análisis forense proactivo: Investigación enfocada en la actividad anómala y maliciosa que no puede ser detectada por las herramientas automatizadas de supervisión de seguridad.

b. Captura y coerción: Alterar la red y las condiciones del punto final para provocar que un atacante inicie una actividad maliciosa susceptible a ser detectada por el seguimiento dirigido de forma intensa.

Los datos y resultados del análisis cibernético y el análisis de inteligencia sobre amenazas permiten que se realicen actividades de Defensa Activa; es decir, un marco que proporciona el elemento de "ejecución" del análisis cibernético e inteligencia sobre amenazas. Esto permite que las estrategias de tercera generación y los casos de uso sean utilizados por los analistas de datos para la creación de modelos a fin de identificar y responder a los ataques cibernéticos.

36%

de las organizaciones cuenta con un programa formal de inteligencia sobre amenazas.

¿Puede integrarse en las operaciones de seguridad?

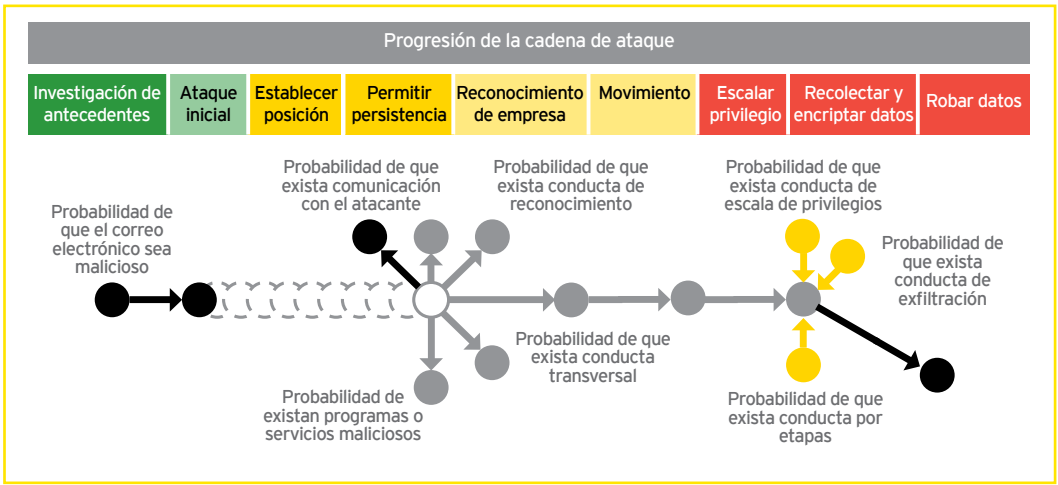
La ciencia de datos, basada en libros de estrategias enfocadas en el negocio y casos de uso identificados, pueden ser aprovechados para aplicar estadística a los eventos, y combinaciones de eventos, a fin de:

1. **Crear herramientas de seguimiento conductual continuo.**
2. **Priorizar eventos para dar respuesta a incidentes.**
3. **Proporcionar una innovación ágil frente a atacantes innovadores.**

Análisis conductual para el monitoreo continuo

La ventaja del análisis conductual permite a las organizaciones extraer y presentar patrones significativos a partir de datos. En el contexto de seguridad, esto ha significado tradicionalmente que se puede extraer normas y patrones a partir de ataques pasados y luego compararlos con los actuales.

Con la evolución de los Centros de Operaciones de Seguridad de tercera generación, el análisis conductual viene extendiendo los usos y capacidades anteriormente aceptadas, a través de la medición de la desviación con respecto a la conducta pasada. Utilizando el modelamiento estadístico, se puede identificar anomalías que indiquen cambios en la conducta de los atacantes. Una ventaja principal de los métodos conductuales es que no requieren de evidencia de comportamiento malicioso pasado y pueden ser autodidactas. Exponga los datos, y estos empezarán a aprender lo que es "normal" versus lo que es "anormal".



La dificultad radica en identificar una conducta extraña que sea consistente con los ataques, no solo una conducta o sino benigna. Es aquí donde la ciencia de datos necesita usar los conocimientos operativos, en la forma de respuesta a incidentes y simuladores de *hacking*, a fin de asegurarse que se está consultando los datos estadísticos de la información apropiada, de forma correcta, para prestar la atención cuando se desencadena un evento inusual que es consistente con un comportamiento de ataque. Es raro encontrar a científicos de datos con la combinación de experiencia en seguridad cibernética y habilidades de modelamiento de datos, por lo cual adquirir esto como un servicio puede ser la prioridad para muchas organizaciones.

Al construir modelos estadísticos que representen conductas pasadas, las organizaciones están empezando a atribuir puntajes a los datos observados actualmente y pilotear los mecanismos de detección del seguimiento de seguridad de tercera generación. Los eventos inusuales disparan alertas que alimentan los tableros de control u otros mecanismos de generación de reportes para identificarlos y entregarlos a los encargados que dan respuesta a incidentes.

35%

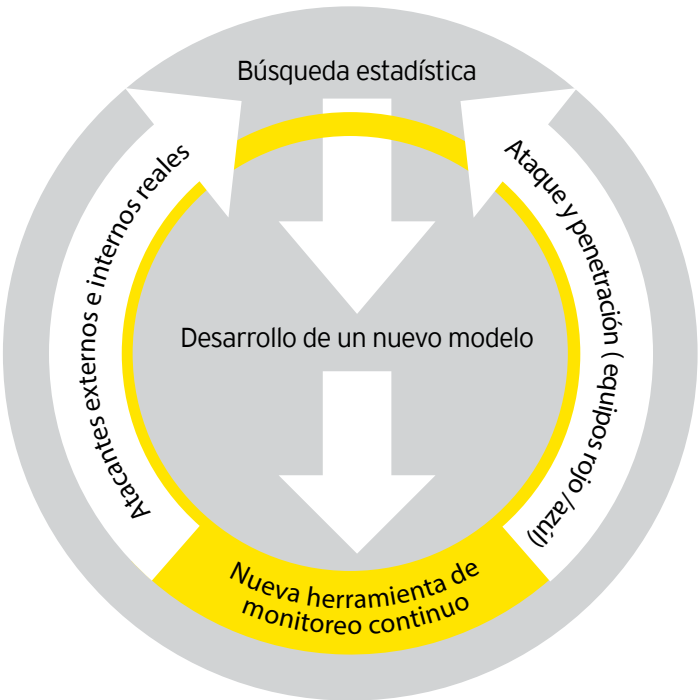
indica que la amenaza de un ataque de día cero ha tenido una alta prioridad en los últimos 12 meses.

61%

de las organizaciones indica que las pruebas de seguridad son una prioridad media o baja.

Búsqueda Estadística

El uso de la analítica permite a las organizaciones extraer y presentar patrones significativos a partir de los datos. En el contexto de la seguridad, esto ha significado tradicionalmente que se puede extraer normas y patrones a partir de ataques pasados y luego asemejarlos con los suministros de datos entrantes.



Innovación Continua

La rapidez con las que innovan los adversarios es mucho mayor que con la que se desarrollan nuevas defensas. Las vulnerabilidades previamente desconocidas, o llamadas de día cero, son comunes. Aún más desafiante es el hecho de que los atacantes solo necesitan identificar un nuevo método de conducta de ataque y evitar la detección, mientras que los defensores necesitan cubrir todos los conceptos de operación posibles – una tarea imposible. Las herramientas defensivas sufren de la necesidad de pasar por los ciclos de ventas de productos que tienen periodicidades anuales, para traer nuevos métodos al mercado. Finalmente la tecnología de red subyacente está cambiando constantemente por debajo de los defensores, con la aparición de la política del "Traiga su Propio Dispositivo" y el "Internet de las Cosas". Existe la necesidad de acelerar las operaciones de defensa, y la ciencia de datos puede ayudar.

54%

de las organizaciones no tiene actualmente un rol o departamento enfocado en el impacto de las tecnologías emergentes sobre la seguridad de la información.

A través de la interacción con los equipos de búsqueda, personas encargadas de responder en caso de incidentes y de realizar las pruebas de penetración, se puede desplegar rápidamente nuevos métodos de detección, actuando directamente sobre los datos operativos a fin de producir nuevas herramientas de supervisión continua e indicadores futuros de ataque. Las organizaciones necesitan poder hacer miles de preguntas acerca de sus datos, determinar cuáles son efectivos y traerlos rápidamente a la producción.

62%

de las organizaciones indica que proteger las tecnologías emergentes (por ejemplo, la nube, la virtualización, la tecnología móvil) es una prioridad media o baja.

"Red Team"

Los términos "equipo rojo" y "equipo azul" se derivan de los juegos de guerra militar tradicionales: los equipos rojos son los atacantes y los azules los defensores. En el uso que le da la seguridad cibernética actual, el equipo rojo es un grupo que desafía activamente una organización para mejorar la eficacia de su seguridad a través de ejercicios específicos que aprovechan técnicas que incluyen las pruebas de penetración y la ingeniería social, entre otros.

Dichos ejercicios deben ser realizados regularmente para supervisar a la organización como un todo y que la arquitectura de la plataforma se encuentre asegurada contra ataques, utilizando técnicas similares a aquellas mostradas por atacantes reales. Las organizaciones necesitan garantizar que todo hallazgo sirva para

retroalimentar el ciclo de vida del desarrollo de nuevos controles para su subsanación.

Ejecutar escenarios de equipo rojo versus equipo azul permite a las organizaciones ver cómo la plataforma cibernética detecta los ataques y evaluar dónde existen oportunidades para modificar o construir nuevos modelos de detección en todo el proceso de ataque. Además de identificar los puntos ciegos potenciales dentro de la red, esto tiene el beneficio añadido de capacitar a la nueva generación de analistas utilizando ejercicios controlados. Esto es especialmente eficaz cuando un miembro del equipo rojo trabaja en conjunto con el equipo azul, notificando al equipo azul sobre el progreso y validando la detección.

La inteligencia del equipo rojo debe tener como fuente una variedad de lugares, incluyendo monografías, presentaciones y foros. Al aplicar esta información a la plataforma, una organización puede determinar cuán efectivo es su análisis de datos y si existe la necesidad de desarrollar nuevos modelos y módulos de detección de anomalías. Las herramientas y metodologías de ataque del equipo rojo están evolucionando más rápido que las herramientas y metodologías defensivas del equipo azul, por lo tanto el trabajo en conjunto entre los investigadores del equipo rojo con los científicos de datos y los buscadores del equipo azul reduce rápidamente el tiempo necesario para generar nuevos modelos y módulos. El equipo rojo puede simular los ataques nuevos dentro de la red para validar la detección de la plataforma.

Conclusión

Los Centros de Operaciones de Seguridad pueden hacer que su negocio sea más seguro en el mundo digital

El entorno continuamente cambiante de las amenazas de un mundo cada vez más digital, desafía las capacidades de defensa incluso de las organizaciones más maduras.

Un COS con buen funcionamiento puede formar el corazón de la Defensa Activa y proporcionar un entorno seguro para que la empresa cumpla con sus objetivos estratégicos principales.

Estamos siendo testigos de la convergencia de un conjunto de habilidades especiales y disciplinas relacionadas con la seguridad cibernética, ciencia y análisis de datos en entornos COS avanzados, donde el todo es más grande que la suma de sus partes.

El *sponsor* detrás de las operaciones de seguridad de tercera generación es un programa integrado de gestión de amenazas cibernéticas. Este programa integra y mejora las capacidades de seguridad existentes de la empresa para lograr una mejor efectividad contra los atacantes persistentes a través de una Defensa Activa. Al implementar y ejecutar un ciclo interactivo con mecanismos incorporados para un aprendizaje continuo y una mejora continua, potenciados por el ciberanálisis y el análisis de inteligencia sobre amenazas, las organizaciones pueden obtener ganancias en eficiencia, control de responsabilidades y capacidades de gobierno. Estas ganancias se traducen directamente en un mejor retorno sobre la inversión de los programas de seguridad, incrementando la efectividad de las operaciones de seguridad y reduciendo la efectividad de los ataques dirigidos.

Preguntas para el Directorio

¿Cuán seguro está usted que su organización no se encuentra actualmente comprometida? ¿Cómo lo sabe?

¿Cuenta usted con las habilidades adecuadas dentro de su equipo para detectar y responder a un ataque cibernético?

¿Está usted maximizando el rendimiento de sus inversiones en seguridad cibernética integrándolas bajo un marco común alineado a su negocio?

¿Su proceso de toma de decisiones se basa en información exacta y dirigida, basándose en un análisis de inteligencia?

¿Está su COS alineado con su estrategia de negocio para asegurar que se mantenga el enfoque en los activos de mayor valor?

¿Cómo puede ayudar EY?

Si usted está diseñando un COS desde cero o está mejorando sus capacidades existentes, EY puede ayudarlo en cada etapa de su implementación.

Nuestro enfoque en el cual integramos el análisis de inteligencia sobre amenazas, la supervisión de seguridad, la respuesta ante incidentes y el análisis de seguridad, reflejan la situación actual de su entorno tecnológico, incluyendo la detección de la conducta de las amenazas y la exposición de sus datos.

Las amenazas continúan evolucionando y su COS también debe hacerlo. Nuestros servicios están diseñados para involucrar a personas con experiencia y procesos eficientes en torno a las tecnologías líderes para proporcionar un COS centrado en el negocio que puede desarrollarse con las necesidades de su empresa y el entorno cambiante de las amenazas.

Contactos | EY Perú

Paulo Pantigoso
Country Managing Partner
Telf: +51 1 411 4418
paulo.pantigoso@pe.ey.com

Consultoría / Advisory

Jorge Acosta
Advisory Leader
Telf: +51 1 411 4437
jorge.acosta@pe.ey.com

Numa Arellano
Telf: +51 1 411 4428
numa.arellano@pe.ey.com

José Carlos Bellina
Telf: +51 1 411 4444 Ax. 16117
jose.bellina@pe.ey.com

Elder Cama
Telf: +51 1 411 4444 Ax. 16102
elder.cama@pe.ey.com

Alejandro Magdits
Telf: +51 1 411 4453
alejandro.magdits@pe.ey.com

Víctor Menghi
Telf: +51 1 411 2121
victor.menghi@pe.ey.com

Cecilia Ota
Telf: +51 1 411 4444 Ax.17355
cecilia.ota@pe.ey.com

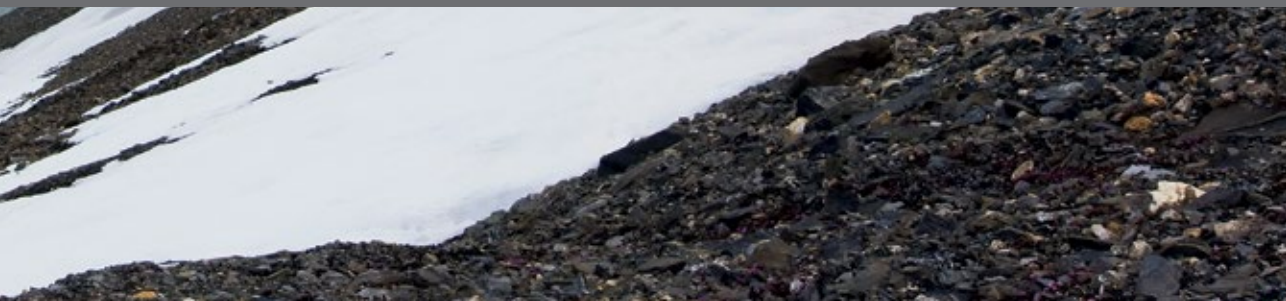
Renato Urdaneta
Telf: +51 1 411 4438
renato.urdaneta@pe.ey.com

Raúl Vásquez
Telf: +51 1 411 4415
raul.vasquez@pe.ey.com

Lima
Av. Víctor Andrés Belaúnde 171,
San Isidro - Lima 27, Perú
Telf:: +51 1 411 4444
Fax: +51 1 411 4445
www.ey.com/pe/es/home

Arequipa
Av. Bolognesi 407,
Yanahuara - Arequipa 040,
Arequipa
Telf:+51 54 484 470

Chiclayo
Av. Santa Victoria 612,
Urb. Santa Victoria, Chiclayo 140
- Chiclayo
Telf: +51 74 227 424
+51 74 227 421



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 criminales 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? Pregunte a EY.

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

EY | Assurance | Tax | Transactions | Advisory

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 ey.com

EY PERÚ LIBRARY

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

/EYPeru
@EYPeru
/company/ernstandyoung
/EYPeru
perspectivasperu.ey.com
ey.com/pe