


# Seguridad de la información en un mundo sin fronteras

Es momento de replantear el tema



*La seguridad de la información busca un equilibrio entre el nivel de seguridad y el costo, y plantea dos preguntas importantes:*

- ▶ **¿Cuáles son las medidas que las compañías deben tomar en el mundo hiperconectado y sin fronteras de hoy?**
- ▶ **¿En qué momento las empresas son lo suficientemente seguras?**

## Contenido

### Es momento de replantear el tema 2

Es tiempo de replantear los programas de seguridad de la información y las estrategias que las compañías utilizan para mantener a salvo sus activos más valiosos.

### Un enfoque de seguridad integrado 3

El nuevo enfoque de seguridad integrado contiene cinco acciones entrelazadas:

- Identificar los riesgos reales 4
- Proteger lo más importante 6
- Optimizar para el desempeño del negocio 8
- Sustentar un programa empresarial 10
- Habilitar el desempeño del negocio 12

### La seguridad de la información en acción 14

En un mundo cada vez con menos fronteras, aproveche la oportunidad para:

- Alinear su estrategia de seguridad con las necesidades de su negocio
- Identificar y proteger su información más crítica
- Fomentar una cultura de confianza y responsabilidad



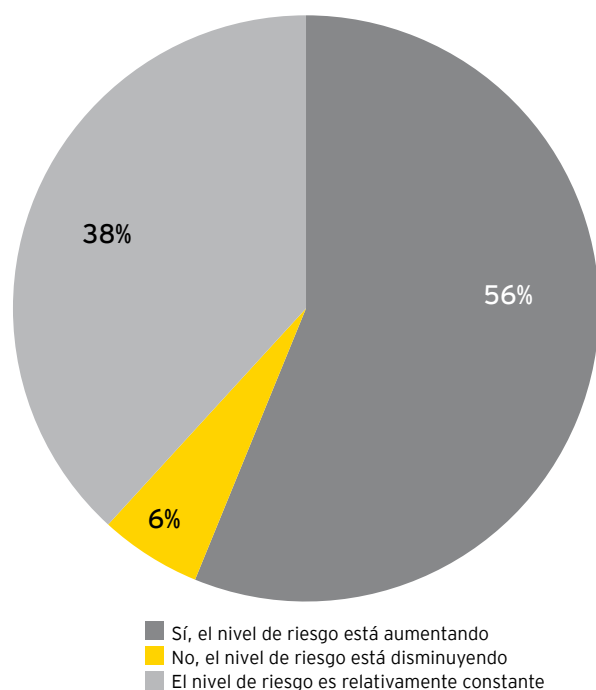
Si su organización se está basando en el pasado para proteger su futuro, su programa de seguridad de la información ya está obsoleto.

## Introducción

# Es momento de replantear el tema

Los modelos de seguridad tradicionales se enfocan en mantener alejados a los atacantes externos. La realidad es que existen amenazas tanto dentro como fuera de la organización. La tecnología móvil, computación en nube, las redes sociales y el sabotaje por parte de los empleados son solo algunas de las amenazas internas que enfrentan las empresas. A nivel externo, no solo se trata del **hacker** solitario que ataca por gusto. En general, el entorno de riesgo está cambiando, como lo vimos en **13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México**.

Debido a las tendencias actuales de utilizar elementos como las redes sociales, la computación en nube y los dispositivos personales móviles en la empresa, ¿ha visto o percibido un cambio en el entorno de riesgo que enfrenta su organización?



Muestra: porcentaje de encuestados

Fuente: 13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México.

Es tiempo de replantear los programas de seguridad de la información y las estrategias que las compañías deben utilizar para mantener a salvo sus activos más valiosos. La seguridad de la información debe estar alineada estratégicamente con la agenda de negocios más general y basarse en la tolerancia al riesgo de una organización. ¿Qué constituye un nivel aceptable de riesgo de seguridad de la información en un entorno donde la propiedad intelectual, información personal del cliente y la marca están en juego? Es una decisión difícil que debe tomarse para formar la base de un programa transformacional de seguridad de la información.

Los avances tecnológicos han creado un acceso a la información que es demasiado grande para las barreras. Por lo tanto, las compañías deben aprender cómo aceptar el cambio de manera segura. Nuestro enfoque de seguridad integrado puede ayudar a su organización a construir un programa para aumentar la confianza con sus clientes, proveedores, socios de negocio y empleados de manera rentable y sustentable.

## Temas para replantear

- ▶ Los modelos de seguridad tradicionales que se enfocan principalmente en mantener las amenazas externas lejos de la organización ya no son eficaces. El nuevo modelo es predictivo y aplica para toda la empresa.
- ▶ Para proteger la información de su compañía, los dueños de los negocios y equipos de seguridad deben identificar la información y aplicaciones más importantes, en dónde se localizan y quién tiene o requiere acceso a ellos.
- ▶ Los ataques son inevitables. Enfóquese en las soluciones que planean, protegen, detectan y responden ante las amenazas. Utilice las medidas de protección adecuadas para la información que está más expuesta.
- ▶ Los fundamentos son tan importantes como siempre, pero deben equilibrarse con la administración de amenazas emergentes.
- ▶ Invierta prudentemente en controles y tecnología para mejorar el desempeño. Considere la posibilidad de subcontratar algunos elementos de su programa.
- ▶ Asegúrese de que las funciones de gobierno sean las adecuadas - convierta la seguridad en una prioridad a nivel del consejo de administración.
- ▶ Aumente las medidas de seguridad al habilitar el uso apropiado de nuevas tecnologías en lugar de prohibirlas.

# Un enfoque de seguridad integrado

## Predictivo y para toda la empresa

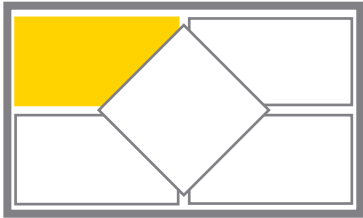
Es momento de cambiar la perspectiva. La seguridad de la información no es un simple ejercicio de cumplimiento. Ninguna solución puede inocular a una red de un ataque y proteger la información no solamente depende del área de TI. En cambio, el nuevo enfoque de seguridad integrado es predictivo y para toda la empresa. Protege de manera proactiva y espera lo peor.

Opta por aceptar ciertos elementos en lugar de prohibirlos. Se enfoca en la confianza y no en la paranoia. A continuación se presentan los elementos de una estrategia transformacional de seguridad de la información que su organización puede utilizar para fomentar la confianza en un mundo sin fronteras.



Si considera que su organización no tiene riesgos reales, entonces no los ha identificado.

## Identificar los riesgos reales



### Identificar los riesgos reales

- Definir la inclinación de riesgo general de la empresa y cómo encaja el riesgo de la información.
- Identificar la información y aplicaciones más importantes, en dónde se localizan y quién tiene o requiere acceso.
- Evaluar el panorama de amenazas y elaborar modelos predictivos que resalten su exposición real.

Los profesionales de seguridad a menudo se quejan de que están demasiado ocupados resolviendo los asuntos que requieren atención inmediata y no tienen tiempo de anticiparse a los problemas que se encuentran a la vuelta de la esquina. Si pretende proteger los activos críticos de su organización, tanto el negocio como los equipos de seguridad deben entender en dónde reside su información (afuera o adentro). Saber qué es lo que su compañía considera como información y aplicaciones más importantes, en dónde residen y quién tiene o podría requerir acceso a ellas, permitirá que el negocio sepa qué áreas del programa de seguridad son las más vulnerables a ataques.

Después de conocer en dónde reside la información, evalúe el panorama de amenazas y elabore modelos predictivos que puedan resaltar su exposición real. A continuación se presentan algunas de las amenazas más relevantes que enfrentan las organizaciones:

- **Amenazas internas.** La reciente publicación de WikiLeaks de los cables diplomáticos clasificados del Departamento de Estado de EE.UU. es un excelente ejemplo de los ataques maliciosos internos. En este caso, un especialista de inteligencia de bajo nivel del Ejército de EE.UU. fue acusado de divulgar información clasificada, lo cual no se controló eficazmente. Pero la advertencia no termina ahí. Las amenazas internas prevalecen aun más que las externas, ya sea accidental o intencionalmente. Durante mucho tiempo las organizaciones no han sido capaces de entender la importancia de las amenazas internas. Este riesgo solamente aumentará si no se atiende en estos momentos.
- **Computación en nube.** Las compañías están trabajando cada vez más con proveedores de computación en nube debido a varias posibles ventajas, incluyendo una inversión inicial considerablemente menor, menos recursos internos de TI con experiencia y costos operativos más bajos. Sin embargo, a pesar de todos los posibles beneficios, los servicios de computación en nube aumentan los riesgos de seguridad y retos reglamentarios ya que la información personal y propiedad intelectual atraviesan las fronteras. Debido a que no todos los países ponen énfasis en la seguridad y privacidad de la información, la tarea de cumplir con muchos de los reglamentos parece desalentadora. Además, surgen inquietudes en torno a las prácticas de seguridad clave que adoptan los proveedores de computación en nube. Aun en las jurisdicciones que valoran mucho la privacidad puede haber excepciones. Por ejemplo, ciertos reglamentos de EE.UU. permitirían que las autoridades tengan acceso (en circunstancias específicas) a la información personal en manos de los proveedores terceros de computación en nube, sin antes notificar al propietario o sujeto de la información.
- **Dispositivos móviles.** La proliferación reciente de los dispositivos móviles orientados hacia el consumidor ha alterado considerablemente el flujo de información tanto dentro como fuera de las organizaciones. Los empleados utilizan con frecuencia teléfonos inteligentes y tabletas multimedia que a menudo son de su propiedad, para acceder a información de la empresa en cualquier lugar y momento. Aunque esto aumenta la productividad de los empleados, conlleva varias amenazas y riesgos. Muchas organizaciones consideran que se deben prohibir estos dispositivos para reducir los riesgos, pero en realidad, estas restricciones solamente aumentan el uso de los mismos. La respuesta real es habilitarlos con las protecciones de seguridad adecuadas.

## Un buen ejemplo

Muchas compañías exitosas de seguridad de la información comienzan por aprovecharse de una pequeña debilidad para lograr un objetivo más grande. Por ejemplo, durante una evaluación reciente de seguridad, nuestro equipo pudo violar una cuenta individual simplemente al utilizar el proceso estándar de cambio de contraseña del cliente e investigar un poco sobre información públicamente disponible. Al descubrir algunas de las respuestas clave a las preguntas (“¿Cómo se llamó tu primera mascota?” y “¿Cuál es el apellido de soltera de tu mamá?”), el equipo pudo cambiar exitosamente la contraseña del usuario y luego ingresar a su cuenta, lo cual derivó en una violación del sistema de RH para el cual dicho usuario tenía autorización. Con base en estos resultados, la organización ajustó su política, procesos y controles para la administración de identidades y accesos.

- ▶ **Ciberataques.** Aunque las compañías han tenido que lidiar con ataques cibernéticos durante años, muchas son actualmente el blanco de ataques más sofisticados y persistentes. Estos se enfocan en un solo objetivo, y a menudo permanecen mucho tiempo hasta que se logra dar en el blanco deseado. Dejan pocas señales de su presencia porque están diseñados para permanecer ocultos y así recopilar toda la información sensible que sea posible. En nuestra experiencia, aquellos que están más en riesgo son las entidades que poseen mucha información o las organizaciones que tienen propiedad intelectual que resulta atractiva en las economías emergentes. Desafortunadamente, muchas empresas no tienen idea de que están en peligro hasta que es demasiado tarde.
- ▶ **Redes sociales.** Ahora más que nunca las personas recurren a las redes sociales. A medida que evoluciona la tecnología, las líneas entre las interacciones personales y profesionales se vuelven menos claras. Los empleados deben entender cómo podría poner en peligro la seguridad y éxito de la organización la forma en que utilizan las redes sociales (en casa o en el trabajo). Desafortunadamente, el extravío de información a menudo es una consecuencia inesperada del comportamiento de un empleado. Las compañías deberán implementar un programa de concientización para los colaboradores en toda la empresa acerca de su responsabilidad personal para proteger la propiedad intelectual de la organización. Las compañías deben garantizar que la seguridad de la información sea responsabilidad de todos.

## Adelantarse a las amenazas

En el mundo de la seguridad actual, el término *adelantarse a las amenazas* implica mucho más que mantener alejados a los malos. Las soluciones de seguridad de la información tradicionales que se enfocan en las amenazas externas podrían exponer a las organizaciones a otras formas de ataque, especialmente desde adentro.

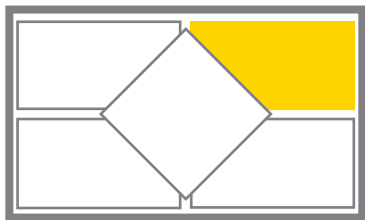
Conozca las debilidades de su programa y adelántese a las amenazas internas y externas a la red, información y marca de su organización:

- ▶ **Definir la inclinación de riesgo de la empresa.** Dicha inclinación depende de su cultura de riesgo. Al entender a fondo la cultura de su organización, podrá alinear la posible exposición al riesgo que está dispuesto a enfrentar.
- ▶ **Identificar la información más importante.** No basta con hacer conjeturas. Debe identificar, inventar y priorizar el valor de la información. Otorgarle un valor a esta con base en la estrategia de negocios general de la compañía le permitirá priorizar los activos más importantes.
- ▶ **Evaluar el panorama de las amenazas.** Las amenazas de seguridad actuales deben enfocarse en conocer en dónde se encuentra la información, quién tiene o requiere acceso a ella y cómo podría estar en peligro. Entender la forma en que se utiliza esta nos ayuda a identificar las amenazas en contra de la misma. Por ejemplo, una organización nacional del cuidado de la salud realizó recientemente investigaciones de campo para determinar la forma en que los empleados y proveedores terceros utilizaban la información. Al observar cómo se compartía esta, la empresa pudo identificar áreas de riesgo de seguridad y tomar las medidas adecuadas.
- ▶ **Desarrollar modelos de amenaza predictivos.** Una vez que su equipo de seguridad identifique las áreas de riesgo, resulta útil repasar los escenarios de este. Estos ejercicios le ayudan a entender y cuantificar la probabilidad de que ocurra una violación en cada área de riesgo específica, el tamaño de las vulnerabilidades y el nivel de daño que podría causar una violación de seguridad.
- ▶ **Determinar los mecanismos de protección adecuados.** Se debe utilizar el modelo de amenazas que fue elaborado para

## Tres preguntas clave

- ▶ ¿Cuál es la cultura de riesgo de su organización?
- ▶ ¿Ha detectado y monitoreado amenazas dentro y fuera de la organización?
- ▶ ¿Ha anticipado nuevos riesgos de tecnología, como dispositivos móviles, redes sociales y computación en nube?

# Proteger la información más importante



## Proteger lo más importante

- ▶ Elaborar una estrategia de seguridad enfocada en los impulsores de negocio y en proteger los datos de alto valor.
- ▶ Aceptar que habrá violaciones - mejorar los procesos para planear, proteger, detectar y responder.
- ▶ Equilibrar los fundamentos con la administración de amenazas emergentes.
- ▶ Establecer y racionalizar los modelos de control de acceso para las aplicaciones e información.

Ya no existe la opción de estar 100% seguros. En cambio, las organizaciones deben crear una estrategia enfocada que proteja la información más importante y que responda rápidamente cuando ocurra una violación. En la *13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México*, analizamos los pasos que las empresas están dando para abordar los riesgos nuevos o que van en aumento. Según los encuestados, los tres controles principales que las organizaciones están implementando son: ajustes a políticas (39%), más actividades de concientización de la seguridad (38%) y técnicas de encriptación (29%).

¿Cuáles de los siguientes controles ha implementado para mitigar los riesgos nuevos o que van en aumento?



Muestra: porcentaje de encuestados

Fuente: *13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México*.

## Un buen ejemplo

Una compañía de petróleo y gas creía que no tenía problemas de fuga de datos. Sin embargo, debido a un ataque que sufrió uno de sus pares, la empresa decidió contratar un proveedor externo para asegurar que su información estuviera segura.

En el segundo día de revisión de Ernst & Young, nuestro equipo descubrió que una jurisdicción extranjera estaba robando información sensible acerca de su propiedad intelectual patentada y vendiéndola en el extranjero. Esta compañía no tenía clientes en esa jurisdicción y no había una razón de negocios válida por la cual los datos estuvieran filtrándose hacia esa dirección.

Con base en los resultados, los cuales sorprendieron al consejo y comité de auditoría, la organización replanteó completamente su enfoque para manejar la información, es decir, cómo proteger esta y a la vez permitir el uso de la misma.



Las compañías inteligentes están cambiando su enfoque para construir capacidades eficaces de detección predictiva y respuesta.

## Detectar y monitorear

Las compañías inteligentes están cambiando su enfoque para construir capacidades eficaces de detección predictiva y respuesta. Esto significa capturar nuevas fuentes de información, almacenar esta durante más tiempo y analizarla para detectar señales de intrusión o actividades anormales que indiquen que está en peligro. Debido a que las amenazas actuales actúan de manera sigilosa, no basta con solamente correr un sistema de detección de intrusiones para señalar las acciones maliciosas conocidas. Sus equipos de seguridad deben poder utilizar indicadores predictivos para analizar las actividades de la red que podrían parecer normales pero que realmente son dañinas.

Una administración de amenazas eficaz únicamente comienza con la detección. Después es importante contar con la capacidad para responder a los ataques al momento de detectarse. Los estudios de referencia demuestran que los equipos de respuesta ante incidentes son una parte cada vez más primordial del equipo de seguridad de la información. Aunque la respuesta ante incidentes anteriormente se limitaba a luchar contra virus y gusanos, los equipos actuales no solo deben tener conocimientos técnicos, sino ser capaces de formar relaciones con las organizaciones pares para compartir información, colaborar con agencias gubernamentales para fines de inteligencia y dirigir equipos globales grandes.

## Prevenir la pérdida de datos

Las herramientas de prevención de pérdida de datos (PPD) trabajan para evitar que las personas con acceso a información privilegiada copien esta a discos extraíbles o le envíen archivos por correo electrónico a un competidor. En este contexto, es importante construir fuertes equipos interfuncionales y establecer una política clara antes de habilitar una herramienta.

Aun así, es fundamental mantener expectativas reales. Las herramientas de PPD mejor implementadas identifican las áreas de riesgo más amplias, y muchas veces evitan la fuga de datos, pero no pueden detener a las personas con acceso a información privilegiada que están decididas a robar información, o a los atacantes sofisticados que se dedican a conseguir propiedad intelectual. Entender estas limitaciones significa que su organización puede darse cuenta del valor al evitar la pérdida de datos accidental y no maliciosa, y al utilizar las herramientas para aumentar la concientización entre los usuarios.

Las herramientas de PPD también son eficaces para detectar y responder. Aun en las empresas que se rehúsan a habilitar el bloqueo de dichas herramientas (por temor a interrumpir los procesos de negocio), estas pueden hacer aportaciones considerables a los esfuerzos de detección más amplios. Sus alertas pueden señalar el trabajo coordinado de robo de datos por parte de personas internas con acceso a información privilegiada, y sus actividades de inventario pueden notificar a los equipos de respuesta acerca de la naturaleza crítica de un activo en peligro.

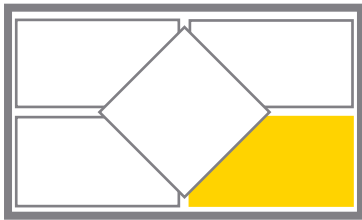
## Optimizar los controles

La organización actual de riesgos de TI se encuentra a menudo en el nexo de los esfuerzos de privacidad, protección de la información y cumplimiento de TI. De hecho, en el estudio *13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México*, 36% de las compañías señala que el cumplimiento reglamentario es una de sus cinco principales áreas de riesgo de TI. Sin embargo, muchas adoptan un enfoque aislado en cuanto al cumplimiento. Las organizaciones líderes adoptan un enfoque más holístico y consolidado respecto al riesgo. Implementar múltiples conjuntos de controles en un marco único de gobierno elimina la duplicidad y simplifica el cumplimiento, y en ocasiones reduce los esfuerzos en un 50%. Un cumplimiento más eficiente significa más tiempo para enfocarse en las amenazas emergentes y en una mejor seguridad.

### Tres preguntas clave

- ¿Ha considerado la posibilidad de automatizar los controles de seguridad?
- ¿Sus equipos de seguridad utilizan indicadores predictivos para analizar las actividades de la red aparentemente normales?
- ¿Sus recursos están enfocados en las amenazas emergentes?

# Equilibrar los fundamentos



## Optimizar para el desempeño del negocio

- ▶ Alinear todos los aspectos de la seguridad (información, privacidad, continuidad física y del negocio) con la organización.
- ▶ Invertir de manera prudente en controles y tecnología - invertir más en gente y procesos.
- ▶ Considerar selectivamente la posibilidad de subcontratar áreas del programa de seguridad operativa.

Las compañías más inteligentes están alineando todos los aspectos de la seguridad (información, privacidad, continuidad física y del negocio) con la organización. También están dando los siguientes pasos para aprovechar al máximo sus gastos, al enfocarse en las inversiones adecuadas, optimizar sus gastos en mecanismos de seguridad primordiales e invertir en los riesgos emergentes.

## Equilibrar las prioridades e inversiones

Una seguridad de la información sólida le da importancia a los fundamentos de seguridad. Sin embargo, muchas organizaciones están invirtiendo tanto tiempo y dinero en operaciones básicas que han descuidado las amenazas emergentes. No hay duda de que los cimientos de un programa de seguridad, es decir, administración de configuraciones y parches, políticas simples con un cumplimiento medido, validación básica de controles de acceso y fuertes inventarios de activos, son cruciales.

También podría ser momento de que la balanza vuelva a estar a favor de la gente en lugar de la tecnología. Cuando se trata de los fundamentos de seguridad de la información, la tecnología por sí sola no es la mejor inversión. El hardware y software se deprecia y se vuelve obsoleto, mientras que la gente aprende y se adapta. Podría resultar fácil pensar que la seguridad de la información es un problema que se resuelve con hardware y software, pero a medida que las amenazas empiezan a evolucionar y superar la tecnología, un personal de seguridad con suficiente capacitación técnica podría ser su mejor mecanismo de defensa. Usted debe reconocer la importancia de invertir en gente dentro de la organización que entienda sobre seguridad de la información (centralizada y descentralizada). Ponga énfasis en una cultura de que “el equipo de seguridad de la información incluye a todos los empleados”. Capacite a todo el personal acerca de sus funciones, alinee al equipo de seguridad con los líderes de negocio clave y busque patrocinadores en las unidades de negocio. Sin embargo, es fundamental maximizar las inversiones que las compañías han hecho en su gente al resaltar en toda la empresa que la seguridad de la información es responsabilidad de todos.

## Un buen ejemplo

Durante el proceso de integración después de una adquisición reciente, una compañía global analizó detenidamente la eficacia general de su organización de seguridad, sus procesos y su tecnología. El análisis de Ernst & Young resaltó muchas áreas que podrían optimizarse, incluyendo:

- ▶ Simplificar sus diversos marcos de cumplimiento y controles al consolidarlos en un marco de gobierno más completo que aborda las múltiples necesidades de cumplimiento al mismo tiempo.
- ▶ Disminuir considerablemente sus gastos en la administración de vulnerabilidades al subcontratar la administración de computadoras de escritorio y las PC.
- ▶ Mejorar las herramientas que utiliza para la administración de identidad y accesos al habilitar nuevos elementos de autoservicio que disminuyen considerablemente las llamadas al Help Desk.

■ Impulse el valor de las inversiones que se encuentra realizando y destine más tiempo a las áreas que tienen mayor riesgo.

## Invertir de manera prudente

El estudio *13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México*, señaló que 35% de los presupuestos de seguridad de la información aumentaron en 2011, un patrón que se ha observado durante varios años. Sin embargo, 94% de los encuestados señaló que su postura de riesgos era igual o peor en comparación con años anteriores. Se requieren nuevas tecnologías para adelantarse a las amenazas recientes, pero podrá aumentar su eficiencia al tener más recursos para adelantarse a las amenazas y al optimizar las tecnologías existentes antes de buscar nuevas.

## Realizar subcontrataciones selectivas

Al subcontratar de manera selectiva las partes más operativas de su programa de seguridad de la información, podrá liberar algunos recursos para aquellas tareas de más alto valor. Al subcontratar aquellos procesos estandarizados, como las operaciones de seguridad, administración de parches y configuraciones, administración de dispositivos y manejo de alertas de primer nivel, el personal interno podrá atender los asuntos más críticos.

## Utilizar la tecnología adecuadamente

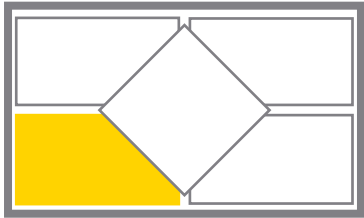
A la industria de la seguridad de la información se le ha acusado de manejarse con base en el miedo, la incertidumbre y la duda. Hay demasiadas organizaciones que utilizan la tecnología como la respuesta a sus problemas de seguridad, pero a menudo fallan sin los procesos contiguos. Además, las compañías a menudo adquieren grandes cantidades de software de estantería (*shelfware*) y no le dan el uso suficiente. Muchas empresas reconocerían que sus herramientas actuales producen grandes cantidades de información que no se analiza, contienen funciones que no se han habilitado o están obsoletas. Para sacarle el máximo provecho a su tecnología, primero construya los casos de uso antes de fijarse en las nuevas funcionalidades técnicas de la herramienta más reciente. Posteriormente, analice la forma en que su organización puede cumplir con dichos casos de uso al minar la información actual, utilizar la funcionalidad latente o volver a realizar una reingeniería de procesos existentes.

## Tres preguntas clave

- ¿Está distribuyendo los gastos entre las prioridades de riesgo clave?
- ¿Ha investigado la funcionalidad latente de sus herramientas existentes?
- ¿Pretende subcontratar algún elemento de su seguridad de la información?

Seguramente cometerá errores. Dese cuenta a tiempo y asegúrese de que sean mínimos.

## Ir más allá del cumplimiento para lograr una seguridad sustentable



### Sustentar un programa empresarial

- ▶ Asegurar que las funciones de gobierno sean las adecuadas - convertir la seguridad en una prioridad a nivel del consejo de administración.
- ▶ Aceptar los riesgos manejables que mejoran el desempeño.
- ▶ Permitir que una buena seguridad impulse el cumplimiento y no al revés.
- ▶ Medir los indicadores líderes para poder identificar los problemas cuando todavía son pequeños.

### Conseguir la atención del consejo para fines de gobierno y determinar la tolerancia al riesgo

Las organizaciones líderes están convirtiendo la seguridad de la información en una prioridad a nivel del consejo. Para este, dos puntos importantes son establecer una base sólida de gobierno de seguridad y un proceso para determinar los niveles aceptables de tolerancia al riesgo para la empresa. Las compañías líderes cuentan con un comité a nivel del consejo para fines de gobierno de TI y supervisión, incluyendo seguridad; así como consejos de riesgo de TI en toda la empresa. Recomendamos proporcionarle actualizaciones periódicas al consejo de administración, por lo menos anualmente, que incluyan los resultados de las auditorías de cumplimiento, incidentes significativos y el estatus de las iniciativas clave.

El consejo también se encarga de determinar que la seguridad de la información esté estratégicamente alineada con la agenda de negocios general de la organización, con base en su tolerancia de riesgo reconocida. Un asunto de alineación es determinar un nivel de inversiones en seguridad que esté acorde con los niveles de tolerancia al riesgo. El costo real de la seguridad es la inversión total en el programa de seguridad más el costo de cualquier incidente relacionado con esta cuando ocurre. Al invertir menos en los programas de seguridad, existe el riesgo de que haya costos más altos vinculados con los incidentes de esta. Por el contrario, al invertir más en dichos programas, el costo total de los incidentes debe disminuir, lo cual resultará a su vez en una reducción en los costos totales de seguridad. Para lograr un equilibrio, es necesario alinear la tolerancia al riesgo aceptada de la organización con los costos totales de seguridad. Los programas de este tipo tienen un costo base, ya que muchas organizaciones descubren que las inversiones adicionales en las medidas de seguridad tienen un nivel de eficacia menor y no darán lugar a una disminución correlacionada en los incidentes de esta.

### Un buen ejemplo

Durante cinco años, una institución financiera había invertido en un programa para identificar y desarrollar tratamientos que remediaron 10 años de riesgos extremos de seguridad de la información. Con la ayuda de Ernst & Young, la compañía realizó actividades para integrar una práctica de administración de riesgos sustentable en el programa bajo un marco acelerado de tres años. El proyecto fue lanzado en una división de la empresa, con el fin de implementarlo en otras dependiendo de su éxito.

En el periodo de tres años al que se había comprometido, la organización fue capaz de:

- ▶ Mejorar su calificación de auditoría de riesgo de seguridad de la información
- ▶ Disminuir más de una docena de riesgos de negocio
- ▶ Liberar capital de auditoría
- ▶ Reducir los riesgos extremos en un porcentaje de dos dígitos

El programa fue tan exitoso que la compañía comenzó a utilizar un programa similar en la región de Asia-Pacífico.



*“Han habido cambios sorprendentes en los últimos años en el entorno reglamentario en cuanto a la protección de la información. Se esperan más leyes y reglamentos en los próximos años. Las compañías responsables buscan adelantarse a estos reglamentos para evitar interrupciones en los procesos de negocio y para trabajar hacia normas y procesos globales y sin fisuras que habilitan, y hasta aceleran, el crecimiento”.*

Nuala O'Connor Kelly, Asesor Senior, Gobierno de Información y Director General de Privacidad, General Electric

## Permitir que la seguridad impulse el cumplimiento

Las organizaciones cuyos programas de seguridad únicamente se enfocan en lograr el cumplimiento tienen carencias en materia de seguridad. Los recientes casos de pérdida de información muestran que las compañías “cumplieron con la norma”, pero no eran lo suficientemente seguras. Ocurrieron violaciones debido a prácticas inseguras y no por la falta de cumplimiento con la norma reglamentaria. A nivel global, los reguladores no han llegado a un acuerdo sobre qué o cuánta información debe protegerse. Debido a lo anterior, los reglamentos no definen a detalle cómo proteger los datos de una organización. Están atrasados en materia de abordar los avances como las redes sociales y los dispositivos móviles, así como la privacidad de la información personalmente identificable. Para estar al día, los legisladores tratan de entender cómo proteger esta en el ámbito público y en el dominio corporativo. Los reguladores también empiezan a exigir que las empresas no solo demuestren que implementaron un programa de cumplimiento, sino que proporcionen evidencia de que funcionó.

Evidentemente, el cumplimiento reglamentario tiene que ser un elemento crítico de cualquier estrategia de seguridad de la información. Sin embargo, no debe ser el único impulsor, sobre todo porque no garantiza que la compañía esté protegida de amenazas actuales o emergentes. Cumplir no es lo mismo que estar seguro. Las normas internacionales de seguridad de la información son una guía útil para impulsar las iniciativas en esta materia, pero el éxito realmente surge de la implementación. Las normas y reglamentos no garantizan la seguridad en la empresa.

## Medir los indicadores líderes

Las métricas de seguridad tradicionales tienden a mirar hacia atrás (los conteos de vulnerabilidad, el cumplimiento con la política, los parches faltantes, el porcentaje de avance de las iniciativas) o se enfocan en estadísticas aparentemente relevantes que tienen poco peso sobre la seguridad de la información real que las compañías buscan proteger. Por

ejemplo, los tableros de seguridad tradicionales podrían reportar la cantidad de alertas generadas por los sistemas de detección de intrusión, las imágenes en los dispositivos de perímetro y el número de veces que se ha bloqueado el software malicioso. Pero es posible que esas métricas no sean relevantes o suficientes. En las audiencias acerca de la eficacia de la Ley Federal de Administración de Seguridad de la Información (FISMA, por sus siglas en inglés), los integrantes del comité parlamentario reconocieron la ineficacia de las métricas basadas en cumplimiento.<sup>1</sup>

Diversos CIO federales y expertos en seguridad reconocieron que a pesar de los miles de millones de dólares invertidos en la medición basada en el cumplimiento para la FISMA, se ha hecho poco por mejorar la seguridad del Gobierno de EE.UU. Desafortunadamente, muchas compañías estadounidenses aún adoptan el mismo enfoque.

Es mejor centrarse en las medidas basadas en resultados. Aunque se deben seguir rastreando las métricas tradicionales, el enfoque debe ser sobre aquellas consideradas críticas que realmente tienen importancia:

- ▶ La cantidad de amenazas reales a la seguridad de la información
- ▶ La cantidad de archivos del negocio que se perdieron por un ataque
- ▶ El tiempo que tarda la organización en recuperarse de una violación

Estas métricas están directamente alineadas con los objetivos de negocio de competitividad e integridad de datos, a diferencia de otras medidas, como la eficacia de los parches o el cumplimiento con las políticas de seguridad.

Estos indicadores líderes le permitirán identificar los problemas cuando todavía son pequeños. Estos errores reducidos le advertirán acerca de las consecuencias inesperadas de las decisiones o acciones de seguridad. Por lo tanto, su compañía podrá: tomar decisiones más inteligentes basadas en riesgo, invertir prudentemente en la administración de riesgos de información y atender de manera eficaz a las áreas de seguridad que representan el peligro más grande.

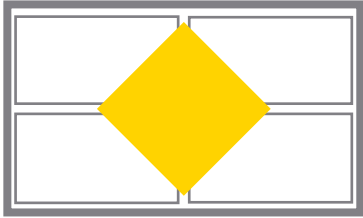
<sup>1</sup> David Perera, *FISMA blasted at House hearing*, FierceGovernmentIT, 24 de marzo de 2010.

## Tres preguntas clave

- ▶ ¿Está tomando riesgos controlados en lugar de eliminarlos por completo?
- ▶ ¿Sus indicadores clave son débiles o fuertes?
- ▶ ¿La información es una prioridad a nivel del consejo?

No prohíba las nuevas tecnologías.  
Utilice las fuerzas del cambio para  
habilitarlas.

## No prohibir las cosas nuevas – aceptar el cambio



### Habilitar el desempeño del negocio

- Garantizar que la seguridad sea responsabilidad de todos.
- No restringir las nuevas tecnologías- utilizar las fuerzas del cambio para habilitarlas.
- Ampliar el programa para adoptar conceptos de administración de riesgos de información para toda la empresa.
- Establecer metas o métricas del programa de seguridad que impacten el desempeño del negocio.

Ante los cambios rápidos, su organización tiene dos opciones: resistirlos o aceptarlos. Apoyamos firmemente la última opción, de acuerdo con nuestro enfoque de seguridad integrado. De hecho, puede utilizar las fuerzas del cambio para crear políticas de seguridad más inteligentes que permitan el uso de nuevas tecnologías en lugar de prohibirlas.

### Garantizar que la seguridad sea responsabilidad de todos

La clave para tener un entorno más seguro es lograr que sus empleados entiendan su responsabilidad personal al momento de utilizar nuevas tecnologías o tener acceso a información corporativa. Esta concientización va más allá de las políticas de alto nivel e incluye ejemplos pragmáticos, como las actividades permitidas y prohibidas al momento de utilizar redes sociales, laptops, tabletas o teléfonos inteligentes. Una lista concreta de “lo que debe y no debe hacerse” es la forma más eficaz de comunicar las políticas y habilitar su uso responsable.

### Habilitar tecnologías más nuevas

Los usuarios quieren utilizar cada vez más dispositivos móviles personales en el trabajo. En lugar de implementar políticas ineficaces en un intento por mantenerlos fuera de este ámbito, analice los controles que pueden proteger, optimizar y habilitar el acceso. Soluciones como trasladar la información crítica a un centro de datos seguro pueden facilitar el acceso en tiempo real a la misma en los dispositivos móviles sin comprometerla. Una gran organización multinacional utilizó recientemente una solución de seguridad que no solo permitió el uso de los dispositivos personales, sino que propició ahorros considerables en relación con el apoyo y adquisición de los dispositivos propiedad de la compañía.

De igual forma, muchas organizaciones bloquean el acceso de los empleados a los sitios de redes sociales en los dispositivos corporativos. Sin embargo, esto no evita que la gente ingrese a las redes sociales, ya sea directamente o por medio de sus dispositivos móviles personales, durante los horarios de trabajo. De hecho, muchos prospectos de reclutamiento jóvenes esperan tener acceso sin restricciones a sus redes sociales, y las empresas que cumplen con esas demandas obtendrán una ventaja competitiva al contratar y reclutar a los mejores talentos.

Los resultados de la *13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México*, muestran que a nivel global las redes sociales no ocupan un lugar prioritario en la lista de retos para la mayoría de los participantes, solo 32% señaló que estas son un reto considerable para poder entregar iniciativas de seguridad de la información de manera eficaz. Esto indica que, aunque la mayoría de las compañías reconocen el hecho de que existen cuestiones de riesgo y seguridad de la información relacionadas con las redes sociales, únicamente unas cuantas han desarrollado un enfoque que equilibrará la oportunidad de negocio con la exposición al riesgo.

## Tres preguntas clave

- ¿Todas las partes interesadas de la compañía entienden la importancia de la seguridad de la información?
- ¿Su empresa está al tanto de las nuevas tecnologías que están presentes en la fuerza de trabajo?
- ¿Su organización cuenta con las medidas adecuadas para crear un *scorecard* de la seguridad de la información a nivel de la compañía?

Para cada uno de los siguientes aspectos, ¿cuál es el nivel de reto relacionado con la implementación eficaz de las iniciativas de seguridad de la información de su compañía?



Muestra: porcentaje de encuestados

Fuente: 13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México.

Sin embargo, en México pareciera que esta tendencia es diferente, ya que 37% de los encuestados señaló este tema como crítico.

Desde luego, para aceptar los cambios podrá ser necesario realizar modificaciones considerables en la cultura de su organización. Tendrá que contar con un buen programa de administración del cambio y un encargado de la ejecución que lo encabece. Comience con el apoyo de los altos cargos y de los ejecutivos que ponen el ejemplo. Siga con un enfoque persistente sobre la gente y comuníquese de forma abierta y honesta, aborde sus inquietudes y céntrese en los beneficios que los cambios traerán consigo.

## Extender los programas de seguridad en toda la empresa

La seguridad de la información debe ser un elemento base de la estrategia general de administración de riesgos de su compañía. Esto fomentará una mayor transparencia en cuanto a los posibles riesgos y permitirá que los equipos de seguridad trabajen conjuntamente con los equipos de mayor riesgo para planear, proteger, detectar y responder ante las amenazas existentes y emergentes. Los equipos de seguridad también tendrán que trabajar con las unidades de negocio para:

- Alinear las funciones de seguridad de la información con los riesgos más importantes para el negocio.
- Coordinar la infraestructura y gente al evaluar continuamente sus niveles de capacidad y brechas, así como la inversión en el desarrollo de habilidades.
- Utilizar métodos y prácticas coherentes que apliquen un enfoque estructurado en cuanto a la administración de seguridad de la información en toda la empresa.
- Asegurar el uso de información y tecnología comunes, lo cual promueve un intercambio congruente de datos acerca de los riesgos clave de seguridad de la información y negocios en toda la compañía.

## Establecer métricas del programa de seguridad que impacten el desempeño del negocio

Cualquier programa nuevo de seguridad de la información tendrá que enfocarse en la medición del valor y la responsabilidad. Por lo tanto, deberá desarrollar métricas que midan el impacto que tiene el programa sobre el desempeño del negocio. Estas métricas deben estar alineadas directamente con los objetivos de negocio general de su organización.

Contar con un cuadro de mando de valor para mantener un registro de sus avances y aportaciones podrá ayudarlo a lograr sus objetivos de desempeño. Al definirse junto con las partes interesadas, servirá como una medida cualitativa del desempeño de la seguridad de la información y del valor entregado a la empresa. Los temas que un cuadro de mando de valor debe incluir son:

- La forma en que la administración del número de incidentes que le dieron a la compañía una exposición externa negativa ha servido para administrar el valor de la marca y limitar el riesgo reputacional.
- La manera en que las medidas de seguridad adecuadas ayudaron a limitar la cantidad de trabajo que se tuvo que rehacer y que, por consiguiente, contribuyeron a los resultados finales.
- La forma en que la comunicación acerca de las medidas de seguridad y privacidad (en sitios web, artículos, con base en certificados) ayudó a fomentar el *e-business* y, a su vez, contribuyó a los ingresos.

## Conclusión

# La seguridad de la información en acción

Al replantear su estrategia de seguridad de la información y utilizar nuestro enfoque de seguridad integrado, su organización podrá prepararse proactivamente mientras espera lo peor; podrá aceptar los cambios en lugar de resistirlos; y podrá enfocarse en la confianza en lugar de la paranoia.

Al hacer esto, su compañía podrá administrar los riesgos adecuados e impulsar el valor al:

- ▶ Entender su madurez en cuestiones de seguridad en el presente y futuro. Saber en dónde se encuentra y en dónde quiere estar sirve para guiar la estrategia.
- ▶ Contar con una estrategia de seguridad de la información basada en riesgos que esté alineada con las necesidades del negocio. Esto permite lograr el cumplimiento y mantener la integridad y confidencialidad de la información crítica.
- ▶ Entender a fondo lo que constituye la información crítica de la organización, en dónde se encuentra y quién tiene o requiere acceso a ella.
- ▶ Buscar medios para medir, monitorear y reportar sobre la eficacia del programa de seguridad y los controles.
- ▶ Hacer énfasis sobre un mejor gobierno de la seguridad de la información.
- ▶ Optimizar los programas de seguridad para obtener eficiencias y reducir costos.
- ▶ Crear una cultura de confianza y responsabilidad entre los clientes, consumidores, proveedores y empleados en un mundo con cada vez menos fronteras.





## Acerca de Ernst & Young

En Ernst & Young nuestros servicios se enfocan en las necesidades y problemas específicos del negocio de cada uno de nuestros clientes, porque reconocemos que cada uno es exclusivo de ese negocio.

La tecnología de la información (TI) es clave para que las organizaciones modernas puedan competir. Ofrece la oportunidad de estar más cerca, más enfocado y de responder con mayor rapidez a los clientes, y puede redefinir tanto la eficacia como la eficiencia de las operaciones. Sin embargo, conforme crece la oportunidad, también aumenta el riesgo. La administración eficaz de riesgos de TI le ayuda a mejorar la ventaja competitiva de sus operaciones en la materia al hacer que estas sean más rentables y al reducir los riesgos relacionados con el funcionamiento de sus sistemas. Nuestros 6,000 profesionales en riesgos de TI recurren a nuestra vasta experiencia personal para brindarle nuevas perspectivas y asesoría objetiva y abierta, dondequiera que se encuentre en el mundo.

Trabajamos con usted para desarrollar un enfoque integral y holístico en relación con sus riesgos de TI o para tratar asuntos específicos de riesgo y seguridad de la información. Entendemos que para poder alcanzar su potencial requiere servicios personalizados y metodologías congruentes. Trabajamos para darle el beneficio de nuestra amplia experiencia en el sector, un profundo conocimiento del tema y las perspectivas más recientes de nuestro trabajo a nivel mundial. Así es como Ernst & Young marca la diferencia.

Para obtener más información acerca de cómo podemos marcar la diferencia en su empresa, favor de contactar a nuestros profesionales.

## Contactos

### **Carlos Chalico**

Tel: (55) 1101 6414  
carlos.chalico@mx.ey.com

### **Erika Saucedo**

Tel: (55) 1101 6412  
erika.saucedo@mx.ey.com

# Material relacionado de liderazgo intelectual

Descargue nuestras investigaciones en [ey.com/mx/publicaciones](http://ey.com/mx/publicaciones) (sección Asesoría)



## ***Asuntos relevantes sobre Protección de Datos Personales para 2011***

Los ejecutivos están invirtiendo más dinero para proteger la privacidad de la información personal. ¿Pero lo están haciendo en el lugar correcto? Lea el reporte de este año para conocer en qué temas de privacidad debe enfocarse en un mundo con cada vez menos fronteras.



## ***13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México.***

En nuestra *Encuesta Global de Seguridad de la Información de 2010*, más de 1,600 participantes de 56 países comparten sus mayores fortalezas y riesgos más críticos en el entorno actual de seguridad de la información.



## ***Un enfoque basado en riesgos para la segregación de funciones***

La segregación de funciones es una prioridad para muchos profesionales, debido en parte a los reglamentos impulsados por controles en todo el mundo y a la responsabilidad a nivel ejecutivo por lograr su implementación exitosa. En este documento se plantea un enfoque práctico y basado en riesgos para lograr el cumplimiento con la segregación de funciones.



## ***Controlar las fugas: manejo de amenazas a la información confidencial***

Durante los últimos cinco años, las organizaciones han experimentado un aumento en el volumen de fuga intencional y no intencional de datos. Esta nueva publicación explica cómo un programa que incluye controles técnicos y de comportamiento puede proporcionarles a los empleados responsables una salida para las inquietudes, mientras se protege la información confidencial de las fugas por parte de personas con malas intenciones.



## ***Cloud computing issues and impacts\****

As mainstream adoption of cloud computing services begins in earnest, there are a multitude of factors that cloud service providers and cloud users must carefully consider. This Ernst & Young report explores critical aspects of cloud computing for all companies (users and providers of cloud services) and consumers.



## ***Countering cyber attacks\****

Traditional information security solutions are not enough to protect against persistent threats and attacks. This updated report discusses the measures organizations should consider to detect and react to successful cyber attacks.

\*Disponibles en [ey.com/informationsecurity](http://ey.com/informationsecurity)



Ernst & Young

Aseguramiento | Asesoría | Fiscal | Transacciones

#### **Acerca de Ernst & Young**

Ernst & Young es líder global en aseguramiento, asesoría, servicios fiscales y transaccionales. A nivel mundial, nuestros 152,000 profesionales están unidos por los mismos valores y un compromiso sólido con la calidad. Marcamos la diferencia al ayudar a nuestra gente, clientes y comunidades a lograr su potencial.

#### **Acerca de los Servicios de Asesoría de Ernst & Young**

La relación entre la mejora en el desempeño y los riesgos es un reto cada vez más complejo y primordial para los negocios, ya que su desempeño está directamente relacionado con el reconocimiento y manejo eficaz del riesgo.

Ya sea que su enfoque sea en la transformación del negocio o en mantener los logros, contar con los asesores adecuados puede marcar la diferencia. Nuestros 18,000 profesionales en asesoría forman una de las redes globales más extensas de cualquier organización profesional, la cual integra a equipos multidisciplinarios y experimentados que trabajan con nuestros clientes para brindarles una experiencia poderosa y de gran calidad. Utilizamos metodologías comprobadas e integrales para ayudarles a alcanzar sus prioridades estratégicas y a efectuar mejoras que sean sostenibles durante un mayor plazo. Entendemos que para alcanzar su potencial como organización requiere de servicios que respondan a sus necesidades específicas; por lo tanto, le ofrecemos una amplia experiencia en el sector y profundo conocimiento sobre el tema para aplicarlos de manera proactiva y objetiva. Nos comprometemos a medir las ganancias e identificar en dónde la estrategia está proporcionando el valor que su negocio necesita. Así es como Ernst & Young marca la diferencia.

Para mayor información por favor visite [www.ey.com/mx](http://www.ey.com/mx)

© 2011 Mancera, S.C.

Integrante de Ernst & Young Global

Derechos reservados

CLAVE: SDI001

Ernst & Young se refiere a la organización global de firmas miembro conocida como Ernst & Young Global Limited, en la que cada una de ellas actúa como una entidad legal separada. Ernst & Young Global Limited no provee servicios a clientes.