Deloitte.

Cambiando el juego en el riesgo cibernético
El imperativo de estar seguro, vigilante y tener capacidad de recuperación *

*Documento original: ***Changing the game on cyber risk.*** **The imperative to be secure, vigilant, and resilient.** 2014 Deloitte Development LLC. Traducido por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia.

Contenido

Introducción

Lo que usted estratégicamente hace para que crezca el negocio o para lograr su misión está en el corazón de los riesgos cibernéticos que su organización enfrenta.

La mayoría de reportes sobre la seguridad cibernética se refiere a un tema común: a pesar de la atención aumentada y de los niveles sin precedentes de inversión en seguridad, el número de incidentes cibernéticos – y sus costos asociados – continúa en aumento. Típicamente señalan la creciente sofisticación de los hackers y de otros adversarios como un problema particularmente insoluble, y algunos deliberan sobre si estar seguro es incluso posible en el actual panorama rápidamente en evolución de los ataques cibernéticos.

Sin embargo, preguntas importantes permanecen sin ser resueltas. En particular: ¿cuáles son las razones subyacentes para esta tendencia y cómo las organizaciones pueden actualmente reversarla para comenzar a ganarle la batalla al riesgo cibernético?

La primera pregunta tiene mucho que ver con su organización misma, y no solo acerca de la sofisticación de los actores externos. Durante las últimas dos décadas, hemos tejido una fábrica de conectividad en nuestra economía y en nuestra sociedad vía Internet – una plataforma que fue diseñada principalmente para compartir información, no para protegerla.

Su organización, sea que funcione en el sector público o en el privado, sin duda se ha beneficiado de esta conectividad – orientando la innovación, la eficiencia, y el desempeño que fueron impensables hace una generación. Probablemente usted la ha usado para transformar las relaciones con clientes y constituyentes, construir nuevas fuentes de ingresos ordinarios, o sobreponerse a las restricciones geográficas. O quizás le permitió a usted obtener datos para darle forma a su estrategia de mercado, acelerar el lanzamiento de productos y servicios, o automatizar diversos sistemas operacionales.

O probablemente también amplió sus capacidades mediante tercerización, asociación, y el uso de contratistas, o le permitió participar en reorganizaciones, fusiones, adquisiciones, y desinversiones. Este alcance digital incrementado adicionó niveles de complejidad, volatilidad, y dependencia de infraestructura que no está completamente bajo su control. Sus esfuerzos para crecer, servir, diferenciar y fluir introducen nuevas brechas y oportunidades que los atacantes intentarán explotar – a causa de que sus adversarios, también, aprovechan el Internet para lograr mucho más, más rápido, y desde cualquier parte. Por cada paso que usted da, ellos estarán cerca. En resumen, Lo que usted estratégicamente hace para que crezca el negocio o para lograr su misión está en el corazón de los riesgos cibernéticos que su organización enfrenta.

Cuando consideramos este vínculo inherente entre negocios, desempeño, innovación y riesgo cibernético, queda claro que proteger cada cosa – quizás no imposible – económicamente no sería práctico y probablemente impediría algunas de sus iniciativas estratégicas más importantes. Algunos incidentes cibernéticos ocurrirán. Cada organización tiene que valorar de manera realista su cambiante perfil del riesgo y determinar qué niveles y tipos de riesgos cibernéticos son aceptables. Administrar su riesgo cibernético no es un demonio necesario, sino un aspecto esencial para facilitar el desempeño óptico del negocio.

Esto nos lleva a la segunda pregunta, que es el tema central de este documento. Principalmente, cómo las organizaciones pueden reversar la brecha creciente entre inversión y efectividad en seguridad en un mundo donde no es factible estar cien por ciento seguro.

Dado que usted no puede prevenir *todos* los incidentes cibernéticos, la disciplina tradicional de la seguridad, aislada de un enfoque más comprensivo basado-en-el-riesgo, no es suficiente para protegerle a usted. Mediante los lentes de lo que es más importante para su organización, usted tiene que invertir en controles de seguridad justificados en términos de costo para proteger sus activos más importantes, pero usted tiene que centrarse con esfuerzo igual – en algunos casos mayor – para obtener más luces sobre las amenazas, y responder de manera más efectiva para reducir su impacto. Mediante un programa continuo para lograr estar *seguro, vigilante, y tener capacidad de recuperación*, usted puede tener mayor confianza en su capacidad para cosechar el valor de sus inversiones estratégicas.

Estar seguro

Usted no puede asegurar todas las cosas de manera igual. Estar seguro significa centrar la protección en los activos sensibles al riesgo que están en el corazón de la misión de su organización.

Los tradicionales controles de seguridad, medidas preventivas, e iniciativas de cumplimiento probablemente han consumido la participación del león de su inversión en la administración del riesgo cibernético, y probablemente usted necesitará continuar – o incrementar – sus niveles de inversión, dado que sus apuestas nunca han sido mayores.

Pero usted puede necesitar repensar sus criterios de decisión. Los actores maliciosos, especialmente los motivados por la ganancia financiera, tienden a operar sobre una base de costo/recompensa; si sus defensas son suficientemente fuertes para *elevar sus riesgos* y el nivel de esfuerzo relativo al *valor* de lo que pueden ganar, es más probable que lleven su atención a otra parte.

El "valor" es un calificador esencial. Dado el alcance y la complejidad de su ecosistema digital, Usted no puede asegurar todas las cosas de manera igual. Estar seguro significa centrar la protección en los activos sensibles al riesgo que están en el corazón de la misión de su organización – las que tanto usted como sus adversarios es probable que estén de acuerdo son las más valiosas.

Entre los elementos más importantes están la infraestructura crítica, las aplicaciones, y los datos, así como también los sistemas especializados de control – pero ellos no son componentes aislados. Son parte de servicios más grandes y cadenas de transacción, de manera que es esencial abordar los puntos débiles en el proceso de negocios de extremo a extremo, con la conciencia de que el personal interno, los vendedores y los socios confiables en cualquier punto pueden ser la fuente de errores o de acciones intencionales que le abran la puerta a los incidentes.

Si históricamente usted ha sub-invertido en seguridad, esto debe ser remediado, pero mejorar la seguridad no siempre se trata de gastar más dinero – y tampoco se trata de comprar las últimas herramientas de seguridad. Muchas organizaciones pueden hacerlo significativamente mejor mediante instaurar mejor disciplina en algunas áreas básicas.

Una es el rastreo y la clasificación de los datos. Muchas organizaciones no saben dónde residen actualmente sus datos sensibles. Probablemente estén ubicados en más lugares que los que usted piensa – tanto dentro como fuera de su organización – siendo vistos y compartidos por más personas que las necesarias. Se debe realizar esfuerzo para racionalizar y controlar el acceso siempre que sea posible.

Otra área común y estrechamente relacionada de debilidad es la administración del activo. Las organizaciones grandes generan enorme cambio sobre una base diaria – nuevos usuarios, nuevos dispositivos, nuevas aplicaciones, y el apoyo para los cambios a la infraestructura subyacente. Si los controles de seguridad no están ajustados para mantener el ritmo, probablemente usted cree agujeros que puedan hacer que su organización esté expuesta durante días, meses – o incluso años.

Una Mirada cercana

La **administración fuerte del activo** es un facilitador importante de las prácticas *seguras, vigilantes, y con capacidad de recuperación.*

Por ejemplo, la reconfiguración y el desmantelamiento apropiados de computadores portátiles y de servidores son críticas para prevenir la fuga de datos. Los procesos maduros mantienen actualizado el etiquetado de los activos críticos que respaldan las áreas de negocio de riesgo alto.

Se puede usar inteligencia junto con tecnologías de monitoreo para priorizar la atención ante las alertas de seguridad – ayudando a los analistas a discernir la diferencia entre un evento menor y uno que potencialmente podría convertirse en una crisis de negocio.

Estar vigilante

Mediante trazar de manera cuidadosa los motivos y la sicología de los adversarios, y considerar el potencial para daño accidental, los estrategas del riesgo cibernético anticipan qué puede ocurrir y de acuerdo con ello diseñan sistemas de detección.

Los ataques más costosos del presente tienden a ser los son muy específicos – por razones específicas. Estar vigilante significa establecer la conciencia de amenaza en toda la organización, y desarrollar la capacidad para detectar patrones de comportamiento que puedan señalar, o incluso predecir, el compromiso de los activos críticos.

Recogiendo terabytes de datos, los centros de seguridad de las operaciones pueden generar diariamente cientos de miles – algunas veces literalmente *millones* de alertas. Los analistas son sobrecargados parcialmente a causa de que la detección está centrada en máquinas infectadas, direcciones maliciosas de IP, o intentos fallidos de conexión. Esos detalles *pueden* ser importantes, pero sin contexto, es imposible conocer si usted está viendo lo que realmente importa.

La actividad maliciosa relativamente aislada del pasado ha cedido el paso a empresas de crimen cibernético bien organizadas y a redes de atacantes políticamente motivados, y algunas veces patrocinados por el estado. Ellos pueden robar datos para ganancia financiera, descubrir planes estratégicos para ventaja competitiva, o interrumpir la infraestructura crítica para causar caos o infringir daño económico. Implacables, sofisticados y pacientes, ponen en escena los ataques durante el tiempo necesario hasta conseguir lo que desean. Algunas veces sus empleados o socios – conscientes o de manera inadvertida – son cómplices.

Sus esfuerzos para estar vigilante comienzan con una descripción sólida de lo que usted necesita para defenderse. A través de todos los sectores de industria hay tendencias de amenaza que son discernibles. Conocer el panorama dentro de su industria es un punto de partida importante que necesita ser complementado con un entendimiento de los riesgos de negocio específicos de su organización. Es un ejercicio amplio examinar quiénes podrían causarle daño a usted, qué los motiva, y cómo es probable que operen. Mediante trazar de manera cuidadosa los motivos y la sicología de los adversarios, y considerar el potencial para daño accidental, los estrategas del riesgo cibernético anticipan qué puede ocurrir y de acuerdo con ello diseñan sistemas de detección.

Este es un desafío de negocios, no solo uno de carácter técnico. Los ejecutivos necesitan entendimiento suficiente del panorama de amenazas para proporcionar orientación sobre el riesgo cibernético. Es luego trabajo de sus equipos técnicos trasladar esto en capacidades operacionales efectivas. Y esas capacidades tienen que ser adaptadas de manera continua. Cada innovación crea nuevas posibilidades de que ocurrirá uso equivocado o abuso. Y por cada innovación, y por cada control nuevo que esté en funcionamiento, los actores maliciosos intentarán encontrar las grietas y ver qué se filtra a través de ellas; y usted tiene que hacer ajustes y anticiparse.

Una mirada cercana

Detectar las amenazas persistentes y específicas requiere colaboración a nivel de toda la organización, y por consiguiente gobierno fuerte.

Primero, dado que requieren acceso continuo a un rango muy amplio de datos – no solo de los dispositivos y sistemas de TI, sino también información de negocios tan diversa como nómina de empleados, patrones de uso del cliente, registros de inventario, registros financieros, y potencialmente datos provenientes de fuentes digitales no tradicionales tales como sistemas de reconocimiento facial, registros de acceso a instalaciones, registros telefónicos, sistemas de control industrial y la lista continúa.

Segundo, los diseñadores de esas capacidades requieren compromiso profundo con los líderes del negocio para entender cuál es la actividad “normal” y cuáles son los indicadores del riesgo.

Una mirada cercana

Los ataques internos maliciosos no son impulsivos. Más bien los individuos se mueven en un continuo desde la concepción hasta la acción, mostrando a lo largo del camino ciertos indicadores de comportamiento. Los actos internos a menudo generan indicadores potenciales de riesgo en tres categorías:

- Acciones virtuales, tales como correos electrónicos enviados y bases de datos accesadas;
- Acciones no-virtuales, quizás ausencias inexplicadas; y
- Descriptores contextuales, tales como accesos de usuario y derechos privilegiados.

La revelación de los empleados en riesgo requiere la correlación de los datos a través de esas categorías a fin de conectar los puntos para descubrir los patrones relevantes con el tiempo.

Tener capacidad de recuperación

Si la respuesta a los incidentes cibernéticos es percibida principalmente como una función técnica, probablemente usted no estará equipado para la acción decisiva.

Sus equipos técnicos manejan muchos eventos de seguridad en el día-a-día, ciertamente rutinarios. Pero algunos incidentes pueden convertirse en serias *crisis de negocio*. Tener capacidad de recuperación significa tener la capacidad para rápidamente contener el daño, y movilizar los diversos recursos que se necesitan para minimizar el impacto - incluyendo costos directos e interrupción del negocio, así como daño a la reputación y a la marca.

Si la respuesta a los incidentes cibernéticos es percibida principalmente como una función técnica, probablemente usted no estará equipado para la acción decisiva sobre si los componentes de sus operaciones estarán o no fuera de línea, qué reportar a las autoridades, y cómo colaborar con el hacer forzoso el cumplimiento de la ley. Usted también puede ser menos ágil en resumir las operaciones normales y menos capaz de administrar la percepción del público, y de los otros *stakeholders* tales como clientes, inversionistas, y reguladores.

Si bien la capacidad de recuperación requiere inversión en el despido de personal basado-en-tecnología y en capacidades de recuperación de desastres, la descripción más amplia incluye el conjunto completo de capacidades de administración de la crisis. Implica TI, por supuesto, pero también varios líderes de negocio y de departamento, así como tomadores de decisión provenientes de las funciones legal, riesgo, relaciones humanas, y comunicaciones. Requiere reglas de juego a través de todas esas entidades, diseñadas por adelantado mediante considerar cómo los escenarios de amenaza podrían impactar los activos críticos y los procesos.

Las reglas de juego y las políticas tienen que estar por escrito, pero es igualmente importante ensayarlas mediante juegos de guerra cibernéticos y simulaciones que reúnan los equipos de negocio y de tecnología. Realizar simulaciones crea mejor conciencia organizacional y mejor entendimiento de las amenazas, mejora el juicio cibernético, y planta las semillas de la "memoria muscular" que ayuda a que los equipos respondan flexible e instintivamente en los escenarios que usted visualizó y las situaciones que podrían preverse.

Finalmente, la respuesta al incidente y la administración de la crisis tienen que alimentar los procesos de mejoramiento continuo. Las organizaciones que tienen capacidad de recuperación se toman el tiempo para absorber las lecciones importantes, y para modificar los aspectos de *estar seguro y vigilante* del programa para emerger más fuertes que antes.

Una Mirada cercana

Los ejercicios de juego de guerra cibernética revelan los problemas comunes que causan demoras en responder tan rápida y efectivamente como lo requeriría una situación real de crisis:

- Los grupos acostumbrados a operar como islas enfrentan desafíos para lograr acuerdos sobre la severidad relativa de un incidente, y por consiguiente de las acciones clave que se necesitan.
- Los roles y las responsabilidades, si bien pueden ser esbozados en un proceso manual, no están bien entendidos.
- La carencia de conciencia respecto de las estructuras que hacen forzoso el cumplimiento de la ley y sobre los procesos legales causan fallas para capturar evidencia forense valiosa.

No funcionará sin gobierno

Un programa seguro, vigilante, con capacidad de recuperación, para el riesgo cibernético, no se refiere solo a gastar dinero de manera diferente – fundamentalmente se trata de un enfoque diferente.

La transformación desde un programa tradicional de seguridad de TI orientado-por-estándares, hacia Un programa seguro, vigilante, con capacidad de recuperación, para el riesgo cibernético, no se refiere solo a gastar dinero de manera diferente – fundamentalmente se trata de un enfoque diferente – y su programa será único para usted. El balance de la inversión en capacidades para *estar seguro, estar vigilante, y tener capacidad de recuperación* variará entre las organizaciones, e incluso será aplicado de manera diferente a las diversas áreas dentro de su organización.

- Dicho esto, los programas *Seguro. Vigilante. Con capacidad de recuperación* tienen algunas características comunes:

  Son liderados por el ejecutivo. Los líderes del ejecutivo tienen que establecer el escenario mediante definir las prioridades de la administración del riesgo cibernético, el apetito por el riesgo, y los mecanismos de *accountability*. El respaldo desde lo alto es esencial en el proceso de reunir las personas para concertar las acciones de los diversos grupos y departamentos para que colaboren de nuevas maneras.
- **Involucran a todos.** Si bien los roles específicos necesitan estar bien definidos, el programa no es responsabilidad de una sola parte de la organización; requiere participación horizontal y vertical amplia, así como cambio comportamental a través de toda la empresa.
- **Son programas, no proyectos.** Si bien usualmente requiere una serie de proyectos para abonar el terreno, *Seguro. Vigilante. Con capacidad de recuperación* es un programa ágil y adaptativo que requiere revisión y mejoramiento continuos de los ciclos para adoptarlos a los cambios en el riesgo de negocio y en los panoramas de las amenazas.
- **Son comprensivos e integrados.** Los elementos de *Seguro. Vigilante. Con capacidad de recuperación* no son islas distintas de actividad; son un conjunto de lentes a través de los cuales cada proceso de negocios esencial y cada iniciativa esencial de crecimiento debe ser evaluado o planeado. Cada uno involucra componentes de personas, procesos y tecnología. Y haciéndolo bien, cada uno mejorará a los otros.
- **Van más allá de sus paredes.** Su ecosistema incluye varios socios, proveedores, y vendedores; los incidentes cibernéticos importantes que directamente los impactan también pueden afectarlos a usted de manera importante.

Esas transformaciones no pueden ocurrir sin gobierno fuerte. Instituir el programa *Seguro. Vigilante. Con capacidad de recuperación* requiere una evolución guiada de manera cuidadosa – cambios en roles, procesos, medidas de *accountability*, métricas de desempeño bien articuladas, y lo más importante de todo, un cambio en la mentalidad a nivel de toda la organización.

[1] RFID Radio Frequency Identification = identificación mediante radiofrecuencia (N del t).

Una Mirada cercana

Es un ser viviente. Cualquier iniciativa donde las áreas del negocio sensibles al riesgo sean facilitadas por activos digitales debe ser consideradas mediante los lentes de *Seguro. Vigilante. Con capacidad de recuperación*. Los ejemplos pueden incluir:

- Un ejecutivo de ventas decide empoderar la fuerza de ventas y los socios del canal con herramientas móviles para las ventas;
- Un equipo de proyecto tiene a cargo la consolidación del equipo y la revisión del acceso a la red corporativa para empleados y contratistas como parte de un esfuerzo importante de realineación organizacional;
- Un director de operaciones jefe decide invertir en nueva automatización basada en RFID[1] para los procesos de fabricación e inventario.

Dando ejemplo

Con el ritmo del clima de hoy, las organizaciones no pueden darse el lujo de retrasar la innovación simplemente porque no pueden estar perfectamente aseguradas. Pero tampoco pueden innovar sin considerar de la manera apropiada los riesgos inherentes que se estén generando.

Dónde comenzar dependerá de dónde está usted hoy, pero si usted determina que está temprano en el proceso de transformación, los siguientes pasos pueden ayudarle a moverse en la dirección correcta:

1) **Coloque en el timón a un alto ejecutivo.** Una situación de crisis requiere un líder fuerte que oriente la acción cohesiva, decisiva. Pero establecer el fundamento requiere que alguien con influencia amplia pueda generar compromiso colaborativo, esencial para el éxito del programa, entre el rango diverso de jugadores – la mayoría de quienes pueden no estar acostumbrados a pensar acerca del riesgo cibernético. La persona a cargo del programa *Seguro. Vigilante. Con capacidad de recuperación* tiene que ser capaz de liderar en esas capacidades, y ser respetado entre el rango amplio de líderes, y a nivel de la junta.

2) **Mapee las amenazas a los activos de negocio que importan.** Cree una matriz de orientación del riesgo cibernético de nivel alto mediante reunir los líderes principales del negocio y los especialistas en inteligencia ante amenazas para de manera preventiva discutir los potenciales actores de amenaza y el personal interno de confianza que podrían generar alarma, el daño que podrían causar, y cómo pueden hacerlo. Mediante estos lentes centrados en la amenaza, identifique las áreas importantes de riesgos cibernéticos no abordados. Establezca su apetito por el riesgo y priorice las áreas que programa que conllevan su estrategia para volverse *Seguro. Vigilante, y Con capacidad de recuperación.*

Lance proyectos de prioridad para las "ganancias" tempranas. Establezca el momento para centrarse en las diversas áreas o iniciativas piloto que de manera directa impacten el éxito del negocio o el logro de la misión, con objetivos que puedan ser medidos, y construidos en procesos de mejoramiento continuo. Mediante mantener el centro de atención y la demostración de los resultados, usted puede plantar las semillas de una cultura de *Seguro. Vigilante. Con capacidad de recuperación* que tenga impacto sostenible, de largo plazo.

3) **Acelere el cambio comportamental mediante incentivos y conciencia basada-en-la-experiencia.** El entrenamiento tradicional en seguridad es un componente importante del programa, pero por sí mismo no es suficiente, tal y como es evidenciado por la serie de violaciones que se remota a computadores portátiles robados, contraseñas débiles, o la falla en seguir protocolos seguros para el desarrollo de aplicaciones. En un entorno de trabajo típicamente ocupado y estresante, el solo manual de política no preparará a las personas para realizar la acción correcta. Por consiguiente, cree algunos escenarios de aprendizaje activo que profundicen el entendimiento del impacto de la actividad del día-a-día sobre la postura de la organización ante el riesgo cibernético, e identifique las oportunidades visibles para reforzar el comportamiento correcto mediante programas que recompensen el hablar, el hacer preguntas, y el logro de los objetivos centrales del programa *Seguro. Vigilante. Con capacidad de recuperación*.

Volverse *Seguro. Vigilante. Con capacidad de recuperación* requiere que la organización acoja un punto de vista fundamentalmente diferente de lo que anteriormente hemos denominado "seguridad." El programa de seguridad de ayer a menudo fue percibido como una carga – un conjunto de restricciones, reglas y obstáculos procedimentales impuestos externamente que impidieron las iniciativas de negocio. El rigor de la

Dando ejemplo

seguridad ha sido enfrentado al progreso, entablando batallas sobre los presupuestos y la oportunidad de las iniciativas estratégicas. Dependiendo de qué prevaleció en cualquier punto dado, el resultado neto a menudo ha sido ya sea innovación imprudentemente riesgosa, o un grado de cautela que conduce a pérdida de oportunidades.

Con el ritmo del clima de hoy, las organizaciones no pueden darse el lujo de retrasar la innovación simplemente porque no pueden estar perfectamente aseguradas. Pero tampoco pueden innovar sin considerar de la manera apropiada los riesgos inherentes que se estén generando. El riesgo cibernético y la innovación están vinculados de manera inextricable; más que subordinar uno al otro, los ejecutivos principales tienen que armonizar esos elementos importantes del desempeño del negocio mediante un programa para volverse *seguro, vigilante, y con capacidad de recuperación.*

Contactos

Contáctenos

Para aprender más acerca de cómo su organización puede volverse segura, vigilante, y con capacidad de recuperación, por favor contacte a:

Edward W. Powers
National Managing Principal | Cyber Risk Services Deloitte & Touche LLP
1633 Broadway, New York, NY 10019
epowers@deloitte.com

Adnan Amjad
Partner | Cyber Risk Services
aamjad@deloitte.com

Kelly Bissell
Principal | Cyber Risk Services
kbissell@deloitte.com

Bethany Larson
Partner | Cyber Risk Services
belarson@deloitte.com

Emily Mossburg
Principal | Cyber Risk Services
emossburg@deloitte.com

Rick Siebenaler
Principal | Cyber Risk Services
rsiebenaler@deloitte.com

Cyber Risk Services industry leaders

Consumer & Industrial Products Sean Peasley, Principal – speasley@deloitte.com

Energy & Resources Adnan Amjad, Partner – aamjad@deloitte.com

Financial Services Vikram Bhat, Principal – vbhat@deloitte.com

Life Sciences & Healthcare Mark Ford, Principal – mford@deloitte.com

Public Sector (Federal) Gordon Hannah, Principal – ghannah@deloitte.com

Public Sector (State) Srini Subramanian, Principal – ssubramanian@deloitte.com

Technology, Media & Telecommunications Irfan Saif, Principal – isaif@deloitte.com

Deloitte Cyber Risk Services Outreach Team
cyberriskinfo@deloitte.com
+1 201 499 0605