PASS Panda Security Summit | The European Cybersecurity Hub

CIBER RESILIENCIA:

LA CLAVE DE LA SEGURIDAD EMPRESARIAL

#PASS2018

Introducción y resumen ejecutivo

Si tecleamos en Google "empresa resiliente" el buscador devuelve, en menos de un segundo, 95.700.000 resultados. Este concepto, definido como "la capacidad de recuperarse rápidamente de las dificultades y terminar siendo más fuerte", es desde hace unos años clave para las empresas que se enfrentan a gran número de riesgos derivados del contexto de la economía global: desde ciber ataques a gran escala, fraudes globales y robo de datos personales hasta el riesgo de efectos adversos de los avances tecnológicos como inteligencia artificial, geoingeniería y biología sintética que causen daño medioambiental, a los seres humanos y a la economía.

Asistimos a una transformación de las relaciones sociales, del tejido empresarial y de las gestiones de los gobiernos. Una transformación que basa su potencial en la tecnología, en los datos y en la inteligencia artificial que recoge, filtra, clasifica y correlaciona datos a gran escala para aprender de ellos y ser capaz de predecir.

Así, la transformación digital afecta en tal magnitud a la vida diaria y al funcionamiento de las organizaciones que, hoy en día, se ha convertido en la fuente de la riqueza de las empresas y de la diferencia competitiva de los estados. Apropiarse de esta riqueza ya no es cuestión de guerras armadas, sino de una "simple" transferencia digital de esa riqueza, de los activos de información, que identifica y diferencia al país. Basta con una ciber batalla que ataque a los ordenadores clave para obtener la información necesaria para derrocar un gobierno o para sustraer su ventaja competitiva.

Ser resiliente es un imperativo, entendiendo la resiliencia como "la capacidad inherente de un organismo, entidad, empresa o estado que le permite hacer frente a una crisis sin que su actividad se vea afectada". No sólo hablamos de recuperación, sino de resurgimiento y empoderamiento tras una situación desfavorable.

En el contexto de la seguridad, la ciber-resiliencia hace referencia a la capacidad de una organización de mantener su propósito principal e integridad frente a la amenaza latente de los ataques de ciberseguridad. Una empresa ciber-resiliente es aquella que puede prevenir, detectar, contener y recuperarse, minimizando el tiempo de exposición y el impacto en el negocio de innumerables amenazas graves contra datos, aplicaciones e infraestructura de IT. Especialmente contra los equipos, donde residen los activos más valiosos para la organización, ya que alcanzarlos supone también atacar la integridad de las identidades y usuarios.

A medida que aumentan los peligros, los enfoques tradicionales para mantener la ciber-resiliencia no funcionan. Muchas entidades sobreviven en estados de equilibrio muy precarios y una alteración, que se puede considerar pequeña en relación al tamaño del organismo o a la importancia de los procesos que ejecuta, puede precipitar una crisis. Para evitar el colapso, la gestión de la ciberseguridad necesita una revisión profunda e implantar nuevos modelos de protección.

Hasta hace poco, las empresas financieras y los gobiernos eran los principales objetivos de los ciberataques. Hoy en día, el desarrollo de los negocios de las empresas de cualquier tamaño y sector depende en mayor o menor medida de Internet y, en consecuencia, la amenaza se ha convertido en universal. Conforme aumentan estos peligros, los enfoques actuales para mantener la ciber-resiliencia no funcionan. La gestión de la ciberseguridad necesita una revisión profunda con nuevos modelos de seguridad.

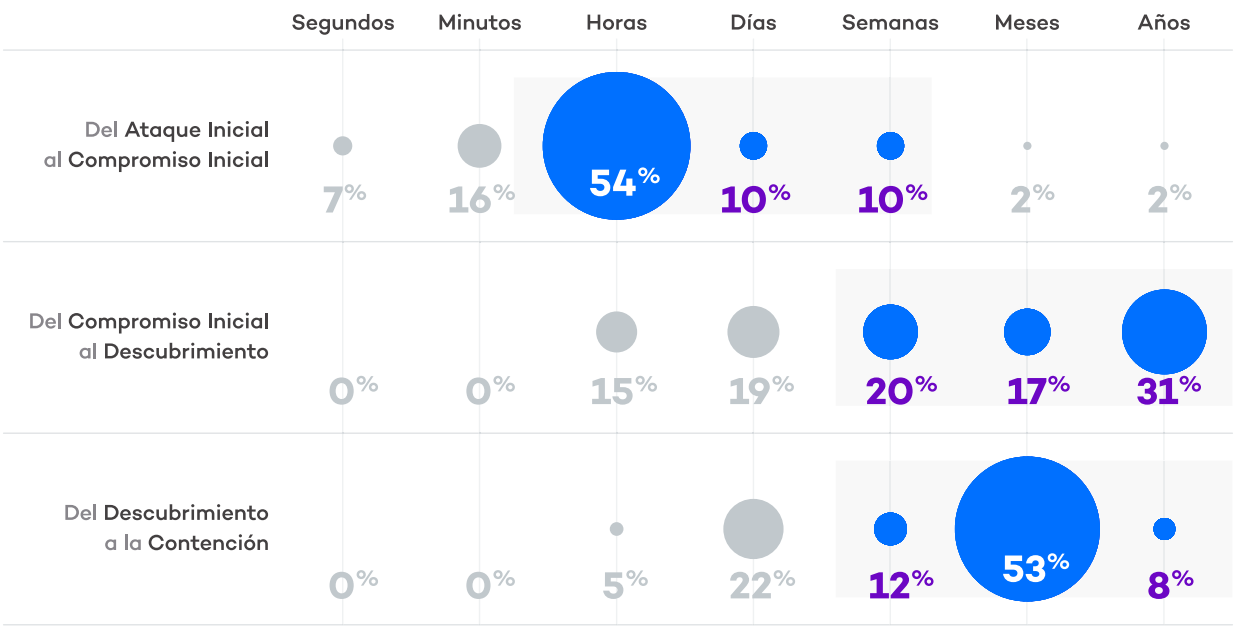
Sin ir más lejos, acabamos de presenciar los casos Meltdown y Spectre, una de las mayores ciber-amenazas recientes, que han hecho patente las vulnerabilidades no sólo del software sino también del hardware. Del mismo modo, entre 2011 y 2014, vivimos cómo las compañías de energía en Canadá, Europa y Estados Unidos fueron atacadas por el grupo de ciber-espionaje Dragonfly. En mayo de 2017, el ransomware WannaCry tuvo como rehenes a organizaciones públicas y privadas en telecomunicaciones, sanidad y logística. También en 2017, el ransomware NotPetya atacó a las

principales empresas europeas en prácticamente todos los sectores.

Pero si bien la conciencia colectiva en esta área se está construyendo, también lo hace la confusión. Las organizaciones y sus ejecutivos están abrumados por el desafío. Según un estudio realizado este año, 2018, por Forrester Consulting para Hiscox[1] a través de una encuesta a más de 4.100 ejecutivos, CISOs, gerentes de IT y otros puestos claves en el Reino Unido, EE. UU., Alemania, España y los países bajos, el 57% de las organizaciones encuestadas afirman estar preparadas para responder a ataques de seguridad. Sin embargo un estudio más detallado a través de preguntas indirectas demuestra que el 73% de las empresas encuestadas están en niveles de madurez bajos y son principiantes en el ámbito de la detección y respuesta a ciber ataques. Solo el 11% de las organizaciones cuentan en sus equipos de seguridad con expertos y, por lo tanto, podrían considerarse como bien preparadas para enfrentar la ciberseguridad.

Para aumentar y mantener su resiliencia a los ciberataques, las compañías deben adoptar una nueva postura: integral, estratégica y persistente con un nuevo enfoque de su programa de seguridad, que puede proteger a las empresas sin imponer restricciones indebidas a sus negocios. Y esta nueva postura debe basarse en fortalecer las defensas preventivas, asumiendo que pueden ser superadas por los atacantes o que estén ya presentes en la organización. Las nuevas técnicas para penetrar las defensas y la ocultación del malware están permitiendo que las amenazas permanezcan en las redes corporativas durante largos períodos sin ser detectadas.

Tampoco pueden olvidarse las amenazas internas. Los ataques de personal con accesos privilegiados suponen una de las mayores amenazas para la



Datos del DBIR de 2016.

[1] 2018 Hiscox Cyber Readiness Report https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

seguridad de la información corporativa y de los datos de tus clientes. Investigaciones realizadas por Ponemon Institute señalan a los hackers y *criminal insiders* como los principales culpables de los agujeros de seguridad y fuga de datos.

El cambio de paradigma hacia una empresa resiliente consiste en evitar que puedan comprometer los activos de la compañía detectándolos antes del daño y respondiendo lo antes posible. Es el momento en el que se materializan tendencias como Threat Hunting, investigación forense para identificar la causa-raíz del ataque, Endpoint Detection and Response (EDR) así como una permanente necesidad de monitorización de los endpoints. La generación de información forense que permita investigar cualquier incidente que tenga lugar en tiempo real es fundamental.

Paralelamente, una empresa madura en resiliencia admite que se producirán fallos, errores, y es consciente de que tiene los medios para restaurar la operación normal para asegurar los bienes y reputaciones. En definitiva: la organización es capaz de salir fortalecida del incidente, aplicando cambios que mejoren su situación de defensa.

La evolución de las amenazas

El Cibercrimen es un negocio atractivo y muy lucrativo. Los atacantes cuentan cada vez con más y mejores recursos –tanto técnicos como económicos- lo que les permite desarrollar ataques cada vez más sofisticados. Todo esto resulta en amenazas más complejas y dinámicas, además de una mayor cantidad de ataques.

Equifax, CCleaner, WPA2, Vault7, CIA, KRACK, NSA, **hackeo de elecciones...** son algunos de los protagonistas del panorama de la ciberseguridad empresarial de los últimos meses. Protagonistas de infecciones masivas, robos de datos, ataques de ransomware, aplicaciones hackeadas para lanzar ataques contra un país, para llevar a cabo ataques dirigidos contra grandes empresas concretas, hasta vulnerabilidades que afectan a miles de millones de dispositivos.

Hay que tener en consideración los estragos causados especialmente por tres eventos recientes. Desde 2011 a 2014, el grupo de ciberespionaje Dragonfly ocupó titulares ampliando rápidamente sus actividades, poniendo en jaque principalmente al sector energético de Norteamérica y Europa. Dragonfly aprovechó dos componentes fundamentales de un programa malicioso, es decir, herramientas de acceso remoto, obteniendo acceso a equipos infectados y controlarlos.

En 2017, **fueron dos ataques los que destacaron especialmente por el impacto y el daño causados: WannaCry y GoldenEye/NotPetya.**

WannaCry apareció en mayo, propagándose y causando estragos en las redes de empresas de todo el mundo, resultando ser uno de los mayores ataques de la historia. Si bien por número de víctimas y velocidad de propagación hemos visto ataques en el pasado mucho más potentes (como el Blaster o el SQLSlammer, por poner sólo un par de ejemplos), lo cierto es que el daño que causaban era colateral a su propagación. Sin embargo, WannaCry es un ransomware con funcionalidad de gusano de red, por lo que cada ordenador infectado acababa con sus documentos secuestrados.

Goldeneye/NotPetya fue el segundo ataque con más repercusión del año, como una **réplica al terremoto que supuso WannaCry.** A pesar de que sus víctimas estaban en principio limitadas a una zona geográfica concreta (Ucrania), acabó afectando a empresas en más de 60 países.

El ataque, cuidadosamente planeado, se llevó a cabo a través de una aplicación de contabilidad muy popular entre empresas en Ucrania, M.E.Doc. Los atacantes comprometieron el servidor de actualizaciones de dicho software, de tal forma que todos los ordenadores con M.E.Doc instalado pudieron ser infectados al momento de forma automática.

Además de cifrar los ficheros, en caso de que el usuario que tiene la sesión iniciada en el ordenador tenga permisos de administrador, el malware va a por el MBR (Master Boot Record) del disco duro. En

principio aparentaba ser un ransomware al estilo de WannaCry, pero tras analizarlo a fondo uno se percata de que realmente **sus autores no tenían intención de dejar que la información secuestrada fuera recuperada**. Días después, el gobierno ucraniano acusó abiertamente a Rusia de estar detrás del ataque.

Y este 2018 no pudo empezar de peor manera en el ámbito de la ciberseguridad que con el **grave fallo de seguridad** encontrado en los procesadores Intel, AMD y ARM. Este fallo de diseño de arquitectura, acompañado de errores en el sistema operativo, cayó como una bomba en el sector tecnológico, y todos trabajaron a contrarreloj para conseguir cerrar las brechas cuanto antes.

El fallo, explotado por el **exploit Meltdown** en arquitecturas Intel, es especialmente crítico desde el punto de vista de **riesgo exfiltración de información sensible** como credenciales, correos, fotos y otros documentos, permitiendo al atacante, desde un proceso malicioso que se ejecuta a nivel de usuario en el equipo o servidor, leer la memoria de otros procesos, incluso la de procesos privilegiados del núcleo del sistema operativo.

Tanto los usuarios domésticos como prácticamente todas las empresas están afectadas, ya que **Spectre** actúa no sólo en equipos, portátiles y teléfonos Android sino también en servidores on-premise y servidores Cloud. Cuanta mayor información crítica se maneje, mayor es el riesgo de ser objeto de un ataque que use esta herramienta.

Y los casos reales no acaban ahí, sino que se extienden a otros gigantes de distintos sectores. Por ejemplo **Apple,** que se vio salpicado por las detenciones en China de 22 personas que supuestamente traficaban con datos de la compañía en el país asiático. Todo parece indicar que se trataba de un trabajo desde dentro, ya que algunos de los detenidos trabajaban para empresas subcontratadas por Apple y tenían acceso a la información con la que los detenidos estaban traficando.

HBO ha sufrido también varios ciberataques en los últimos meses. En uno de ellos le comprometieron servidores robándole episodios completos aún no estrenados de diferentes series de televisión, así como información interna.

InterContinental Hotels Group (IHG) fue víctima de robo de información de sus clientes. Si bien la empresa dijo en febrero que el ataque únicamente había afectado a una docena de sus hoteles, se ha sabido ahora que tenían TPVs (Terminales de Punto de Venta) infectados en más de 1.000 de sus establecimientos. Entre las diferentes marcas de hoteles que posee el grupo se encuentran Holiday Inn, Holiday Inn Express, InterContinental, Kimpton Hotels, y Crowne Plaza.

Sabre Corporation es una empresa norteamericana que gestiona reservas para 100.000 hoteles y más de 70 aerolíneas de todo el mundo. Un atacante consiguió las credenciales para acceder a uno de los sistemas de reserva de la compañía, accediendo a información de pago y detalles de reservas gestionados desde el mismo. Este sistema en concreto gestiona las reservas de particulares y agencias de viajes para 35.000 hoteles y establecimientos de alojamiento. Estuvieron comprometidos desde el 10 de agosto de 2016 al 9 de marzo de 2017, 7 meses.

Pero la mayor brecha de seguridad del año –y de las peores de la historia- llegaría algo más tarde, cuando se supo que el gigante especializado en informes crediticios, **Equifax,** había sido comprometido. Ahora la compañía ha advertido que el cómputo total de afectados asciende hasta los 147,9 millones. La pregunta es: ¿se podía haber prevenido semejante ataque? Sí. **Equifax dejó la puerta abierta a los cibercriminales al no actualizar Apache Struts,** el framework de desarrollo de aplicaciones web. No haber parcheado esta vulnerabilidad permitió que los hackers expusieran los números de seguridad social, direcciones postales e incluso números de los carnés de conducir de millones de personas. Esto demuestra que no cumplir con medidas básicas de seguridad como parchear el software que emplea la empresa puede tener consecuencias colosales.

Con casos reales como estos, no es de extrañar que el 75% de las empresas (según una reciente encuesta de McKinsey[2]) considere que la ciberseguridad es una prioridad para el correcto desarrollo de su actividad. La preocupación por estar preparados ante un ciberataque se extiende a industrias como la bancaria y la automotriz, de las que se podría pensar que estarían preocupadas por otros grandes cambios y riesgos que han surgido en ambos sectores en los últimos años. Hablamos de una amenaza universal y horizontal.

La amenaza es demasiado importante y los atacantes que los originan están creciendo tanto en número como en sofisticación demasiado rápido.

Para aumentar y mantener su resiliencia a los ciber-ataques, las compañías deben adoptar una nueva postura: integral, estratégica y persistente con un nuevo enfoque de su programa de seguridad, que puede proteger a las empresas sin imponer restricciones indebidas a sus negocios.

Esta nueva postura, debe basarse en fortalecer las defensas preventivas pero asumir que los atacantes pueden superarlas y estar ya presentes en la organización o ser parte de la misma organización (Insiders). El cambio de paradigma consiste en evitar que puedan comprometer los activos de la compañía detectándolos antes del daño y respondiendo lo antes posibles. Paralelamente una empresa resiliente debe ser capaz de salir fortalecida del incidente, aplicando cambios que mejores sus situación de defensa.

Retos de las organizaciones en su objetivo de ser Ciber-resilientes

Todo organismo, empresa, organización o estado se ve sometido a tensiones derivadas de eventos, cambios e incidentes que se producen en su entorno, y también que se generan en su interior. Estas situaciones de estrés son nuevos retos cuya resolución afectarán a los procesos de la organización hasta la normalización y automatización de la gestión de la situación de estrés inicial.

En el ámbito de la seguridad en las organizaciones, la situación de estrés descrita en el capítulo anterior requiere de una reacción que suponga un nuevo enfoque en el programa de seguridad en toda la organización. Las empresas deben identificar los activos con mayor valor y establecer un nuevo modelo de gobernanza de la seguridad que centralice, en un equipo central de seguridad, experto y entrenado a reaccionar, la supervisión de todos los esfuerzos de ciberseguridad en toda la empresa. Es el momento de que la cabeza de este equipo gane visibilidad y participe en la toma de decisiones de la organización, formando parte del equipo ejecutivo.

Más amenazas, más intensas

En Estados Unidos ya con la Administración Bush en enero de 2008 se inició la Iniciativa Nacional Integral de Ciberseguridad CNCI. Esta iniciativa Introdujo un enfoque diferenciado, como identificar amenazas de ciberseguridad existentes y emergentes, encontrar y bloquear las vulnerabilidades cibernéticas existentes, y aprender a los actores que intentaban obtener acceso a los sistemas de información federales. El presidente Obama emitió una declaración de que “las ciberamenazas son uno de los desafíos de seguridad económica y nacional más graves a los que nos enfrentamos como nación” y que “la prosperidad económica de Estados Unidos en el siglo XXI dependerá de la ciberseguridad[3]”.

[2] https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world

[3] https://www.es.w3eacademy.com/wiki/State_security

Moving towards cyber *resilience*

The capacity to recover quickly from difficulties and end up stronger.

7%

In 2018, global information security spending is projected to rise by just 7% to $93bn, while the surface area of attack is increasing exponentially.

Invest in cyber security

Without investment, the readiness gap will only intensify.

36%

Only 36% of cyber security professionals have a direct reporting line to the CEO.

Gain a seat at the table

Without greater visibility, cyber security needs will continue to be deprioritised.

35%

By some estimates, only 35% of cyber security professionals vet ecosystem partners for cyber-integrity and preparedness.

Build a more robust ecosystem

Threat detection is crippled without sufficient vetting.

1.5m

The global cyber security workforce is expected to have over 1.5m unfilled positions by 2020.

Improve the talent pipeline

Hire and train more talent.

1/2

Cyber security professionals estimated that over half of threat alerts are improperly reprioritised by systems and must be manually reprioritised.

Make threat detection more accurate

Systems must be honed for an increasingly dangerous digital environment.

Figura 1. El avance tecnológico indudablemente está impulsando cada vez al crecimiento de las empresas. Las organizaciones y el mundo en general están más comunicadas que nunca y el ritmo de desarrollo tecnológico actual es el más avanzado que haya existido. Esta interconectividad y avances tecnológicos traen tanto oportunidades como riesgos.

En diciembre de 2017, la administración del presidente Donald Trump publica un documento sobre estrategia nacional[4] en el que se mencionan problemas de ciberseguridad docenas de veces, y no rehúye nombrar a los países que probablemente usarán redes de endpoints como arma contra los EE. UU.

En este documento se afirma específicamente que los hackers informáticos y los gobiernos de Rusia, China, Corea del Norte e Irán desestabilizan la economía y amenazan la infraestructura crítica de la nación, y que Estados Unidos disuadirá, defenderá y, cuando sea necesario, derrotará a los Threat Actors que utilicen ciberataques contra los Estados Unidos.

Es una realidad: en todo el mundo, la amenaza de los ciberataques está creciendo tanto en cantidad como en intensidad y la rápida e imparable evolución de la transformación digital ayuda a crear nuevas oportunidades para los hackers. Algunas cifras son claros síntomas de esta tendencia tan acusada, como:

- 10 millones de nuevos dispositivos se conectan a nuestro mundo cada día. Se estima que el 2020, los dispositivos interconectados serán 20,8 billones[5].

- Las organizaciones están invirtiendo hasta $500 millones en ciberseguridad[6] y aun así, el 50% de los CEOs de compañías con beneficios de más $500M no se sienten preparados a enfrentarse a ciberataques con garantías[7] y el 82% de los directivos están preocupados o muy preocupados por la ciberseguridad[8].

- En todo el mundo, se crean más de 100 mil millones de líneas de código anualmente, generando millones de puntos vulnerables en los equipos y servidores.

- Muchas empresas informan sobre miles de ataques cada mes, que van desde lo trivial hasta lo extremadamente serio.

- Varios miles de millones de conjuntos de datos se violan anualmente.

- En 2017, los piratas informáticos producen alrededor de 120 millones de nuevas variantes de malware. A día de hoy el número total de software malicioso registrado por AV-TEST es de cerca de los 800 millones[9].

[4] https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

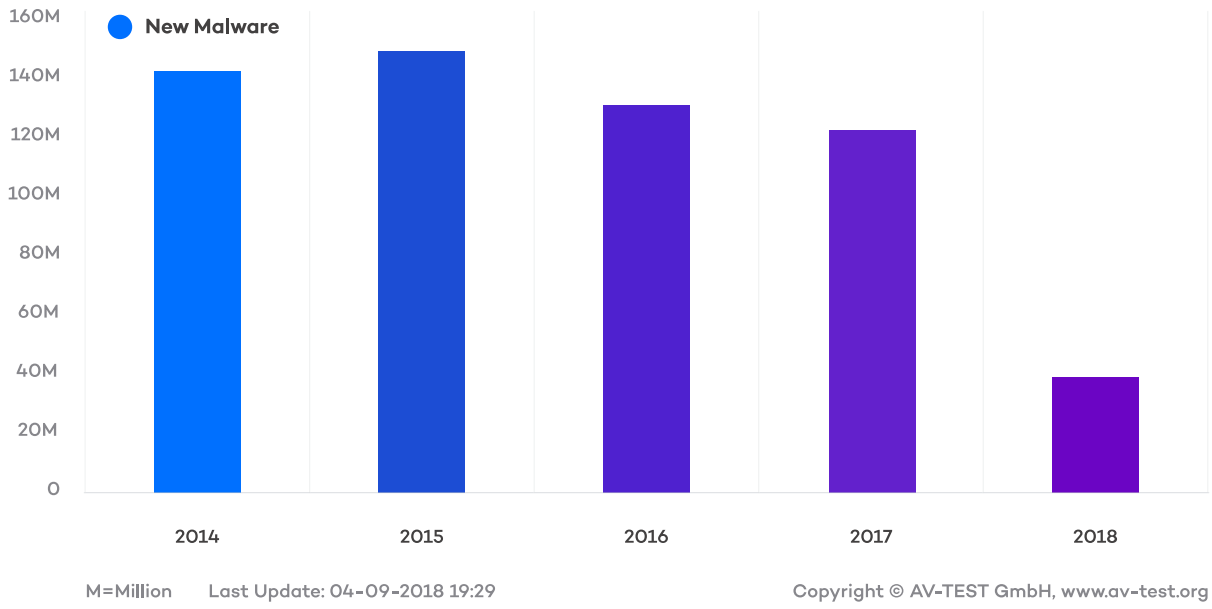
[5] https://www.isaca.org/chapters7/Monterrey/Events/Documents/20172408_Ciberseguridad_Fundamental_Trans_Digital.pdf

[6] https://cybersecurityventures.com/cybersecurity-market-report/

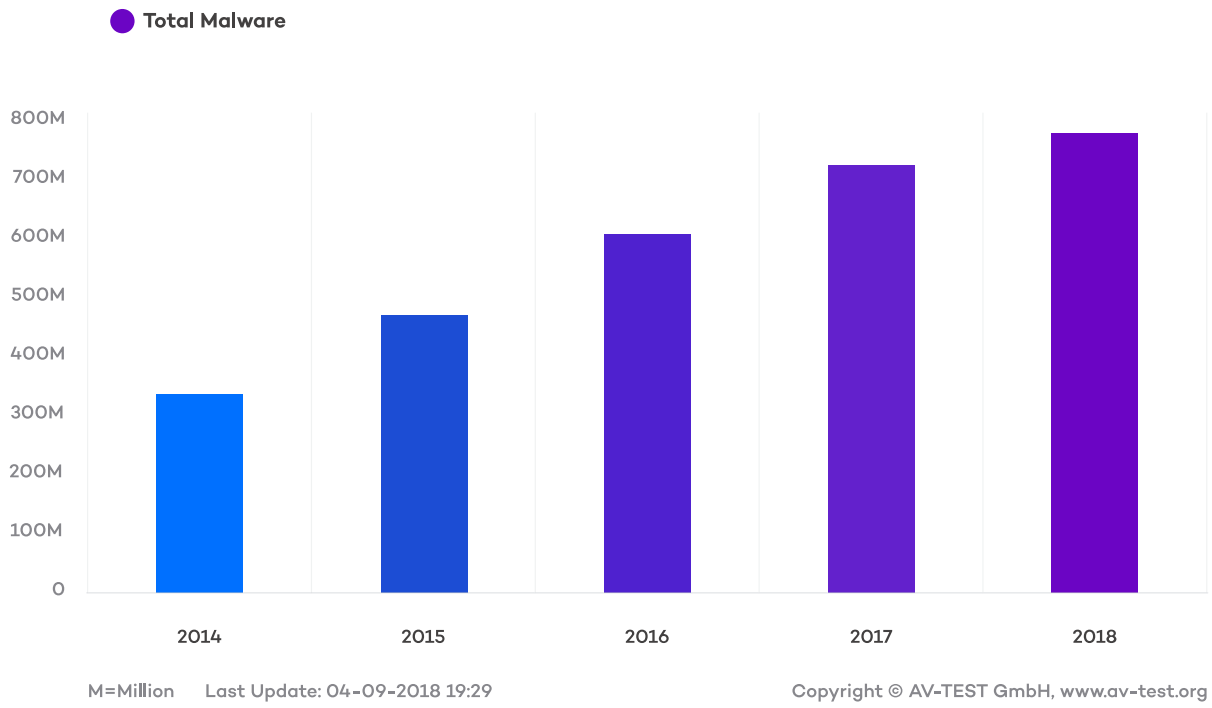
[7] Global CEO Outlook 2015 – KPMG. https://assets.kpmg.com/content/dam/kpmg/pdf/2015/08/global-ceo-outlook-2015.pdf

[8] ISACA/RSA Conference State of Cybersecurity study

[9] https://www.av-test.org/en/statistics/malware/



J.P.Morgan Chase & Co. duplicó su presupuesto anual de ciberseguridad de $ 250 millones a $ 500 millones en 2017. Bank of America declaró tener un presupuesto ilimitado a la hora de combatir el Cibercrimen.



https://www.av-test.org/en/statistics/malware/. Actualización del 9 de abril de 2018.

Paradójicamente, la mayoría de las compañías que fueron víctimas de NotPetya y de WannaCry probablemente hubieran dicho que estaban bien protegidas en el momento de los ataques. Incluso cuando una empresa no es un objetivo principal, corre el riesgo de sufrir daños por malware y ataques contra software ampliamente utilizado. Y a pesar de todas las nuevas defensas, las compañías todavía necesitan alrededor de 191 días en promedio para detectar un ataque encubierto, mejorando algo los 201 días que las organizaciones tardaban en detectar la brecha en 2016[10]. No imaginemos el daño que un atacante no detectado puede hacer en todo ese tiempo.

La Encuesta de SANS Institute de 2016 sobre respuesta a incidentes[11] reveló que el 21% de las organizaciones tenía un MTTD (Mean Time to Detect) de dos a siete días, y solo el 29% podía detectar un incidente en 24 horas o menos. El mismo estudio señala que solo el 18% de las organizaciones podría pasar de la detección a la respuesta (MTTR) en un día o menos. Peor aún, el 38% de la encuesta admitió que, por lo general, no responden en menos de una semana.

Según el estudio sobre la importancia de la resiliencia para fortalecer la situación de seguridad en las empresas de Ponemon Institute, publicado en marzo de 2018, la severidad y el volumen de incidentes de seguridad que las empresas están experimentando incrementa el tiempo necesario para resolverlos.

Como se muestra en la figura 1, extracto del estudio sobre ciber resiliencia de Ponemon Institute, el 64% de las empresas encuestadas

FIgure 13. How has the volume and severity of security incidents changed in the past 12 months?

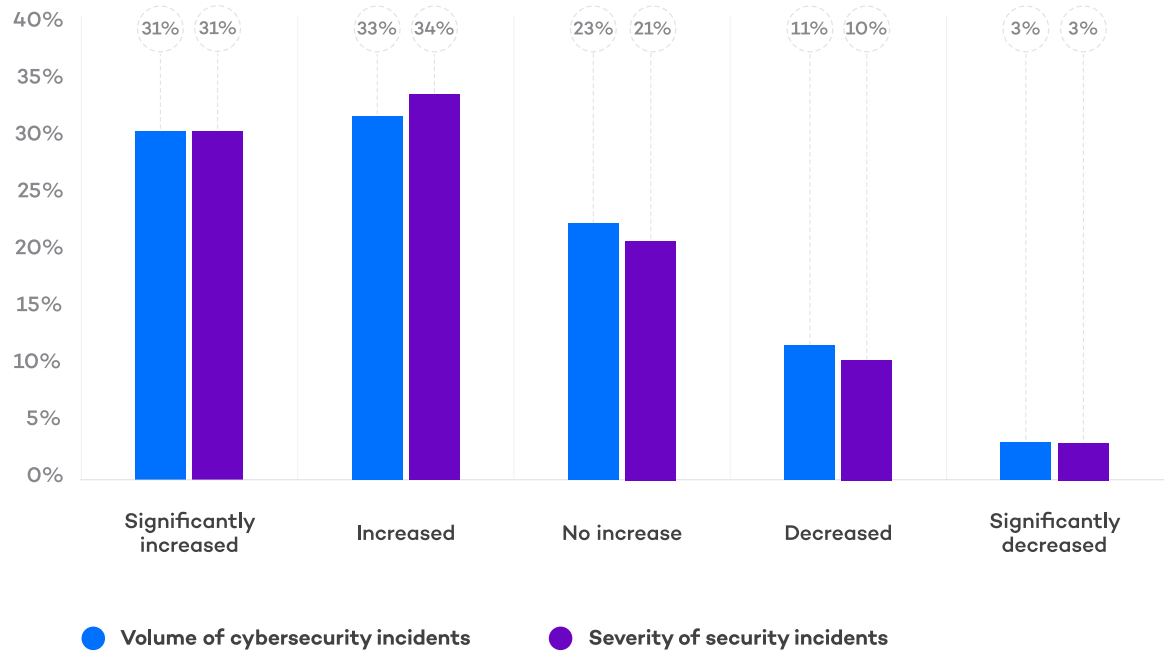


Figura 1. Evolución del volumen y severidad de los incidentes de seguridad en los últimos 12 meses según el estudio de Ponemon Institute de marzo del 2018

[10] 2017 Cost of Data Breach Study (Ponemon Institute for IBM Security)

[11] https://www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047

indican que el volumen se ha incrementado y el 65% de ellas indican que la severidad también. Este incremento en volumen y severidad tiene un efecto negativo en el tiempo de detección y respuesta que ha aumentado significativamente. En la figura 2, se muestra que 57% de las empresas encuestadas dice que el tiempo se ha incrementado.

Complejidad de la infraestructura IT

La creciente complejidad hace que las empresas sean más vulnerables. Mientras los cibercriminales perfeccionan sus habilidades, las empresas se vuelven cada vez más digitales, abriendo nuevas puertas a vulnerabilidades y ciberataques. Los activos que van desde diseños de nuevos productos hasta redes de distribución y datos de clientes ahora están en riesgo. La conectividad digital también se está volviendo cada vez más compleja, utilizando una simple conexión digital para unir a miles de personas, innumerables aplicaciones y servidores, estaciones de trabajo y otros dispositivos. Los activos de las organizaciones están ahora más expuestos.

Algunos errores comunes

La ciberseguridad corporativa lucha por mantener el ritmo vertiginoso de la evolución del ciberriesgo[12], en muchos casos con un enfoque erróneo y una postura poco eficiente. Algunas malas praxis, extendidas en las organizaciones, son:

- Delegar el problema al departamento de IT. Muchos ejecutivos tratan la ciberseguridad como un problema técnico y lo delegan al departamento de IT. Esta reacción, que tiene parte de explicación en que la ciberseguridad presenta muchos problemas técnicos, no tiene en cuenta que defender un negocio es diferente de proteger servidores. La defensa de un negocio requiere un sentido del valor en riesgo, derivado de las prioridades del negocio; el modelo de negocio y la cadena de valor; y la cultura de riesgo, roles, responsabilidades y gobierno de la compañía.

FIgure 14. In the past 12 months, how has the time to detect, contain and respond to a cyber crime changed?

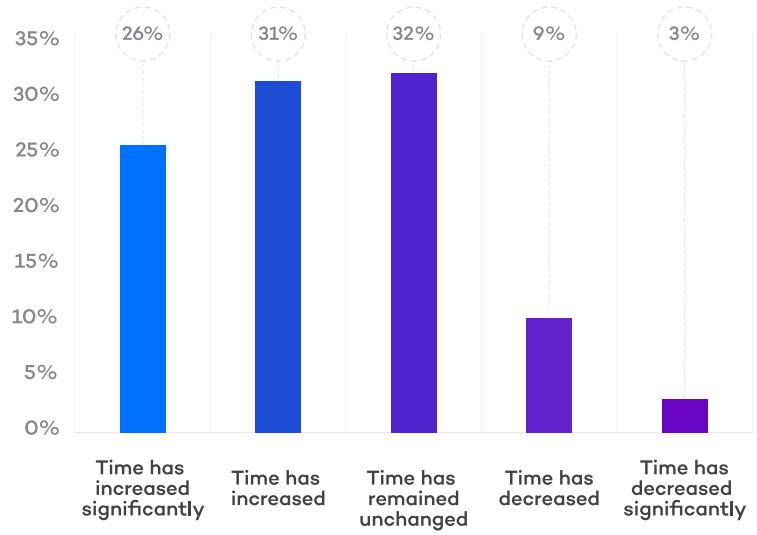


Figura 2. Evolución del tiempo medio de detección y respuesta ante incidentes de seguridad en los últimos 12 meses según el estudio de Ponemon Institute de marzo del 2018

[12] El Instituto AV-TEST registra más de 250,000 nuevos programas maliciosos todos los días.https://www.av-test.org/en/statistics/malware/

- El departamento de IT por sí solo no puede abordar la ciberseguridad, que debe ser tratada como una cuestión corporativa.

- La moda de los "hackers" de alto perfil- o recursos expertos para resolver el problema-. Otras compañías asumen que la amenaza desaparecerá si contratan suficientes "hackers" de alto perfil. Pero incluso los mejores profesionales no tienen la posibilidad de anticipar y defender todos los ataques contra los dispositivos en una red compleja. La solución requiere de expertos, sí, pero también de tecnologías y procesos bien engranados y entrenados. Esto implica inversión a medio plazo y sostenible en el tiempo y toma de conciencia e involucración de todos los departamentos de la compañía y de dirección en el riesgo y sus implicaciones.

- Tratar el riesgo como un problema de cumplimiento de las regulaciones que aplican. Algunas compañías introducen nuevos protocolos de seguridad y checklist de verificación aparentemente cada dos días. Pero estos esfuerzos a menudo provocan un enfoque indebido en el cumplimiento formal, en lugar de una resiliencia real.

Adopción de una postura de ciber-resiliencia en toda la organización

Con este panorama complejo y real y la intención de las compañías de proteger del mejor modo posible el negocio, ¿cómo podemos conseguir ese enfoque más adaptativo, complejo y colaborativo en la lucha?

La ciberseguridad debe ser tratada como un problema de gestión del riesgo corporativo, no como un problema enquistado en IT. Los elementos clave de su gestión incluyen:

- Priorizar los activos más valiosos de la organización.

- Priorizar, conocer y entender a los adversarios y amenazas más relevantes para cada organización.

- Conocer e implantas las mejores defensas preventivas contra las amenazas actuales y potenciales.

- Estar preparado para cuando los adversarios consigan sobrepasar todas las tecnologías de seguridad y detectarlos, contenerlos y remediar sus acciones lo antes posible para minimizar el daño corporativo.

- Adoptar una postura de crisis continua buscando activamente amenazas que hayan entrado en el entorno corporativo y detectar aquellos puntos vulnerables que pueden ser utilizados por estas para reducir la superficie de ataque.

- Gestionar a nivel corporativo la comunicación de la situación de violación.

- Definir y ejecutar constantemente iniciativas que minimicen el riesgo y así volver a empezar con el ciclo de mejora continua en la gestión de la seguridad corporativa.

La adaptación es esencial. La organización, los procesos, las tecnologías, herramientas y servicios de seguridad deben revisarse y ajustarse a medida que evolucionan las amenazas en un proceso de mejora continua basada en desconfianza. El ser resiliente implica que esa adaptación se ha de realizar en el mínimo intervalo de tiempo, a la máxima velocidad, incluso en tiempo real.

Enfoque completo de la gestión de la ciber seguridad en las empresas

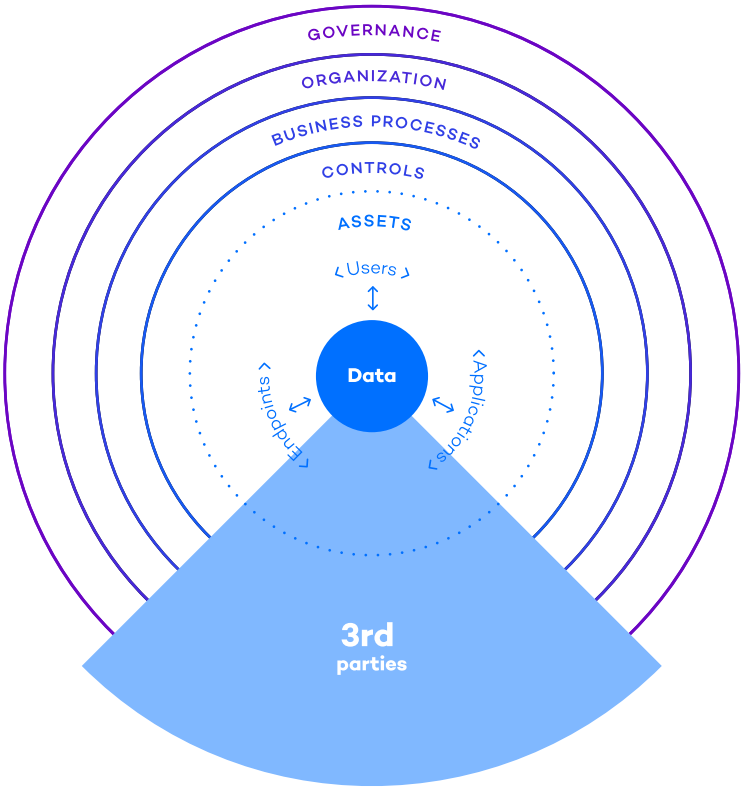


Figura 4. Enfoque completo de la gestión de la ciber-seguridad en las empresas.

Las empresas deben buscar y mitigar su riesgo en todos los niveles. Crear un registro completo de todos los activos, desde datos a aplicaciones, y monitorizar todas las acciones que se realizan con ellos es un proceso largo y tedioso, pero necesario. Las empresas deben aprovechar las herramientas y los servicios que automatizan estas tareas de perfilar, catalogar, y monitorizar sus activos (humanos, datos, infraestructura) para una prevención y/o detección precoz de los adversarios.

Entrar en la dinámica del "ciclo de resiliencia".

Las organizaciones necesitan entender y adoptar el proceso de "ciclo de resiliencia" ayudando a los equipos de seguridad a construir continuamente sobre la experiencia de las amenazas bloqueadas y/o detectadas. Esto requiere que aprendan y se adapten a las fases clave de resiliencia:

- **En fase de pre-incidente**, a través de la capacidad de prevenir y resistir mejor a las amenazas, incluidas las tecnologías avanzadas que detectan malware conocido pero también desconocido o zero-day.

- **Durante su ejecución**, al reaccionar rápidamente con la detección, la contención y la respuesta ante eventos repentinos que amenazan a la organización para minimizar su impacto en el negocio; aprovechando los nuevos paradigmas que surgen a raíz de la capacidad de monitorización y visibilidad que las soluciones de Endpoint Detection and Response (EDR) aportan.

- **En fase de post-incidente**, al absorber los impactos mientras se continúan logrando los objetivos estratégicos de seguridad y reconstruyendo el entorno operativo de forma que se eliminen las futuras fuentes de amenaza de interrupción. Lo que se denomina reducción de la superficie de ataque.

Prevención, detección y respuesta.

Asumir que tarde o temprano cada organización se verá comprometida por un ciberataque. En ese momento, el tiempo de detección y de respuesta al incidente es crítico. Debe buscar un equilibrio entre responder y recuperar el nivel de servicio para el negocio lo antes posible y analizar el incidente, el origen del ataque y establecer medidas para evitarlo en el futuro, incrementando la capacidad de resiliencia de la organización.

Como decíamos en la introducción, la ciber-resiliencia se refiere como la capacidad de una organización para mantener su propósito principal e integridad frente a la amenaza de los ataques de ciberseguridad. Una empresa ciber-resiliente es aquella que puede prevenir, detectar, contener y recuperarse, minimizando el tiempo de exposición y el impacto en el negocio, de innumerables amenazas graves contra datos, aplicaciones e infraestructura de IT. Especialmente contra los endpoints donde residen los activos más valiosos para la organización y contra la integridad de las identidades y usuarios.

Aunque seamos conscientes de que la prevención total no está nunca garantizada, las empresas deben esforzarse a minimizar el coste de los ciberataques fortaleciendo la prevención en fases

Assets	Threats	Controls
Data	• Data breach • Misuse or manipulation of information • Corruption of data	• Data protection (eg, encryption) • Data-recovery capability • Boundary defense
People	• Identity theft • “Man in the middle” • Social engineering • Abuse of authorization	• Controlled access • Account monitoring • Security skills and training • Background screening • Awareness and social control
Endpoints	• Malware	• Control of privileged access • Monitoring processes • Malware execution prevention • Network controls (configuration, ports) • Inventory • Secure configuration • Continuos vulnerability assessment
Applications	• Manipulation of software • Unauthorized installation of software • Misure of information system • Denial of service	• Email, web-browser protections • Application-software security • Inventory • Secure configuration • Continuous vulnerability assessment

Figura 5. Riesgos y controles a implementar en todos los niveles, desde los datos y las entidades hasta los endpoints y las aplicaciones que se ejecutan en estos.

de pre-ejecución, evitando que el atacante ejecute código malicioso en los puestos y servidores. Igual de importante es complementar la estrategia de ciberseguridad con una rápida detección y respuesta en fases de ejecución y post-ejecución, para minimizar el impacto en el negocio conteniendo al atacante, identificando el daño, restableciendo los sistemas para poder operar lo antes posible con normalidad a la vez que identifica las debilidades y puntos vulnerables para corregirlos y evitar así el ataque en el futuro.

Implantar procesos continuos de detección de anomalías en el comportamiento de usuarios, endpoints y aplicaciones.

Cuando se trata de minimizar el impacto en el negocio, el tiempo que transcurre desde que el atacante consigue superar los diferentes sistemas de seguridad, hasta que es descubierto, se contiene su ataque y se responde, es el aspecto decisivo en el coste del incidente.

La monitorización, la visibilidad de lo que sucede en los endpoints y las tecnologías que permiten la automatización del proceso de detección e investigación permiten reducir drásticamente este tiempo detectando comportamientos anómalos o maliciosos en los perfiles de los usuarios, las aplicaciones y los dispositivos, que son sintomáticos de la presencia de un hacker en los sistemas.

La gestión del ciberriesgo exige un gobierno colaborativo integral.

Muchas empresas distinguen entre la seguridad física y de la información, entre IT y Operaciones, entre la gestión de la continuidad del negocio y la protección de datos, y entre la seguridad interna y externa. En la era digital, estas divisiones son obsoletas. La responsabilidad dispersa puede poner en riesgo a toda la organización. Hay que reducir las redundancias y acelerar las respuestas para aumentar la resiliencia en general.

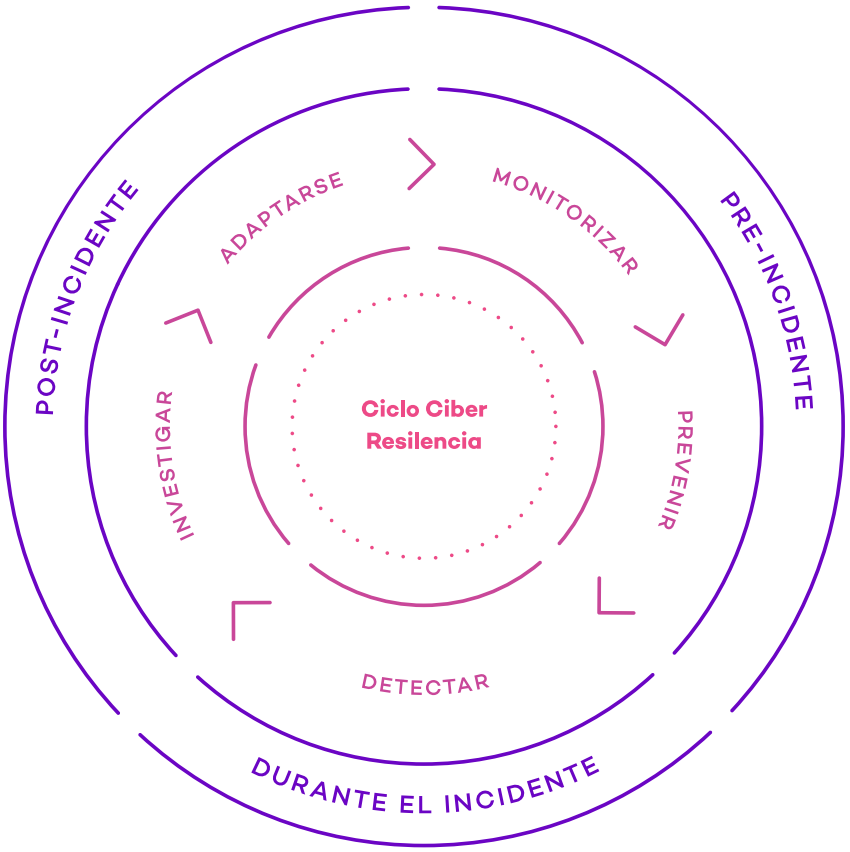


Figura 6. El ciclo de mejora continua de la ciber-resiliencia que toda organización debería de desarrollar e implantar.

La siguiente figura, extraída del informe de Gartner del 28 de enero del 2018: "Improve Operational Resilience Through a More Collaborative Incident Response Process" ilustra las áreas de ciclo de gestión y respuesta a un incidente donde es necesaria la colaboración y coordinación – Las cajas en azul – y las funciones donde aplican las capacidades específicas de cada departamento, operaciones y seguridad – Las cajas en rojo – con el objetivo de detectar y responder en el menor tiempo posible a la vez que se identifican las áreas de mejora:

Las empresas que se adhieren a estos principios tienden a ser mucho más resistentes a la mayoría de los ataques que el resto de las empresas.

Incident Handing

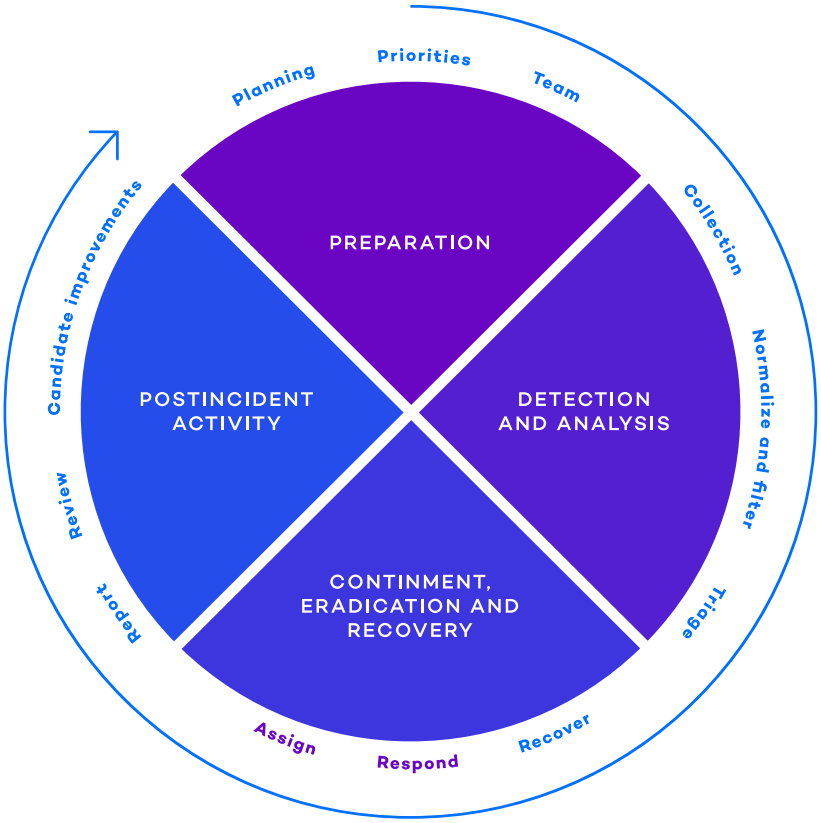


Figura 7. Coordinación entre equipo de Operaciones y Seguridad a la hora de gestionar un incidente de seguridad. Gartner: "Improve Operational Resilience Through a More Collaborative Incident Response Process". 25 de enero 2018. Analistas: Matthew T. Stamper, Kenneth Gonzalez.

¿Cómo es el grado de ciber-resiliencia de mi compañía?

Como parte del estudio sobre resiliencia de IBM y Ponemon Institute, "The Third Annual Study on the Cyber Resilient Organization"[13] realizado este año, se identificaron algunas características que comporten aquellas organizaciones con un alto grado de ciber- resiliencia.

Las empresas deben evaluar cuál es su situación respecto a estas características y tomar las medidas oportunas para reducir la distancia actual frente a lo ideal. Las medidas a adoptar pueden ser múltiples, de diferente índole y adoptando las tecnologías, soluciones y servicios que los vendors de seguridad y proveedores de servicios habilitan con una puesta en marcha inmediata, sin requerir una gran inversión inicial y que cuyo coste se amortiza a corto plazo al reducirse significativamente los costes operaciones derivados de los incidentes y violaciones de datos.

Las empresas con un alto nivel de ciber-resiliencia, se caracterizan por:

1. **Tener un programa de ciberseguridad con altos niveles de madurez** definido, totalmente o al menos parcialmente desplegado en toda la organización y en continua mejora. Según el informe de SANS Institute "Behind the Curve? A maturity Model for Endpoint Security"[14] , donde se define el modelo de madurez en términos de seguridad endpoint, una organización en estados altos de madurez es capaz de prevenir los ciberataques antes de que puedan ejecutarse. O hacer cambios en los sistemas y afectar a los endpoint, detectar aquellos ataques que han podido superar las soluciones de seguridad desplegadas, informar sobre el estado del incidente, remediar y evitar la propagación de nuevos ataques en la empresa. En definitiva, disponen de un programa de seguridad desplegado en la organización basado en la defensa proactiva mejorando sustancialmente la resiliencia general de la organización.

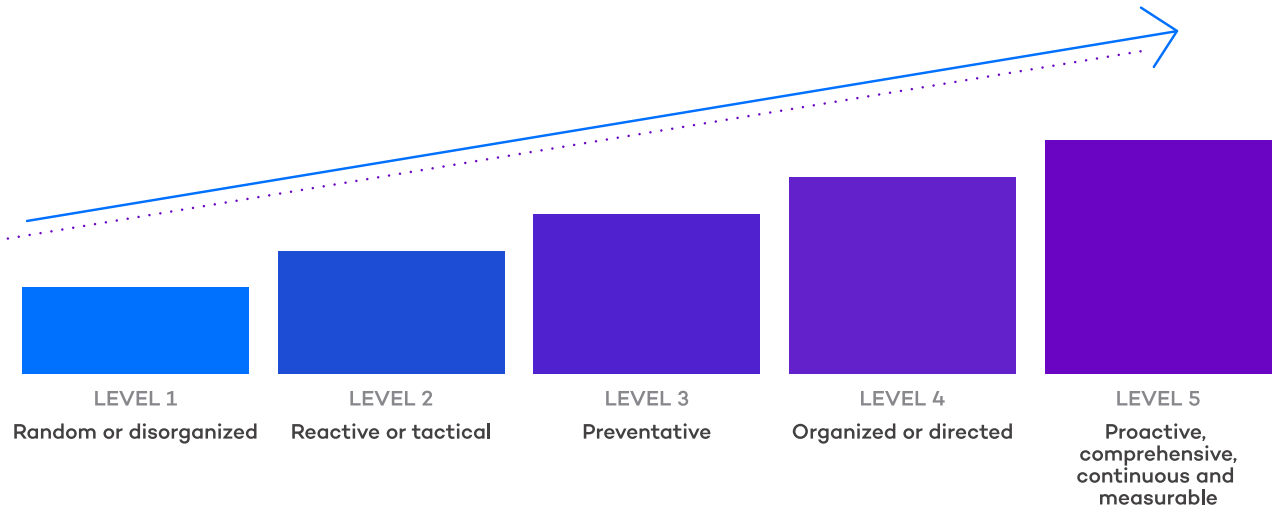


Figura 8. Modelo de Madurez de seguridad en puestos y servidores según SANS Institute, donde se definen los 5 niveles de madurez de las organizaciones con respecto del programa de seguridad desarrollado e implementado.

[13] http://info.resilientsystems.com/2018-ponemon-cyber-resilient-organization-study

[14] http://info.resilientsystems.com/2018-ponemon-cyber-resilient-organization-study

Las organizaciones altamente ciber-resilientes han desarrollado capacidades robustas de prevención, detección, contención y recuperación ante un ciber-ataque.

Según describe el estudio de Ponemon Institute sobre resiliencia, las empresas más resilientes son aquellas en donde se han desarrollado especialmente las capacidades preventivas, de detección de ataques y de respuesta.

FIgure 22. Organizations confident in preventing, detecting, containing and responding to a cyber attack

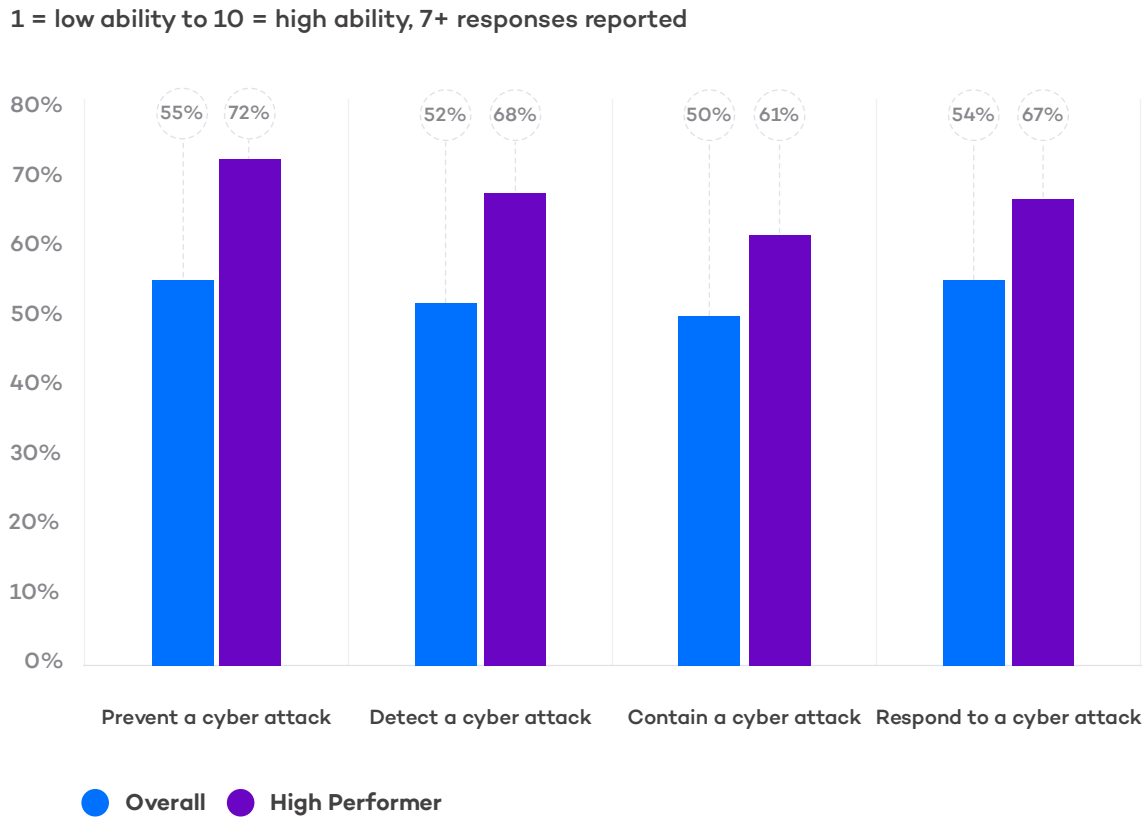


Figure 9. Ponemon Institute: relación entre ciber-resiliencia y capacidad de prevención, detección, contención y respuesta

Las empresas altamente ciber-resilientes han desarrollado un plan de respuesta a incidentes de ciberseguridad (CSIRP: Cybersecurity Incidents Response Plan)

Este plan está fundamentado en una monitorización y correlación continua de eventos recogidos por sensores en los dispositivos de red y/o en los endpoints, así como mecanismos de detección, investigación y respuesta automatizada y/o gestionada por expertos de seguridad, threat hunters.

What best describes your organization's cybersecurity incident response plan (CSIRP)

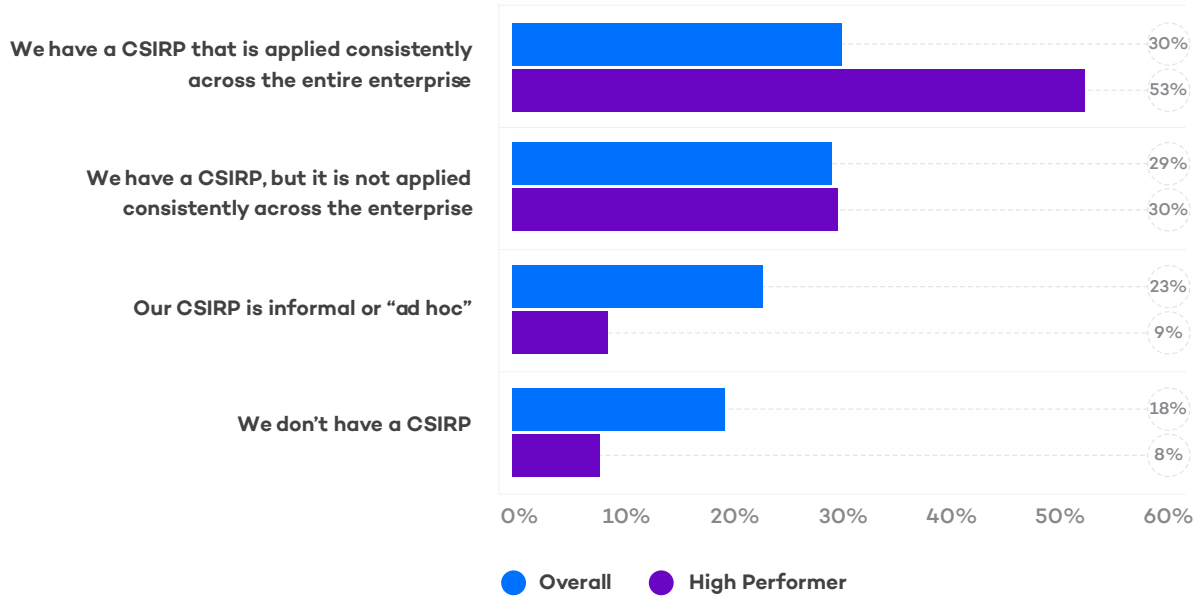


Figure 10. Ponemon Institute: relación entre ciber-resiliencia y la implantación de un plan de respuesta a incidentes de ciberseguridad

Es más, casi todas las empresas con un alto nivel de ciber-resiliencia consideran imprescindible disponer, dentro del equipo interno de seguridad o a través de un SoC externo, de personal altamente cualificado en ciberseguridad como parte del plan de respuesta a incidentes.

It is very important to have skilled cybersecurity professionals in their CSIRP

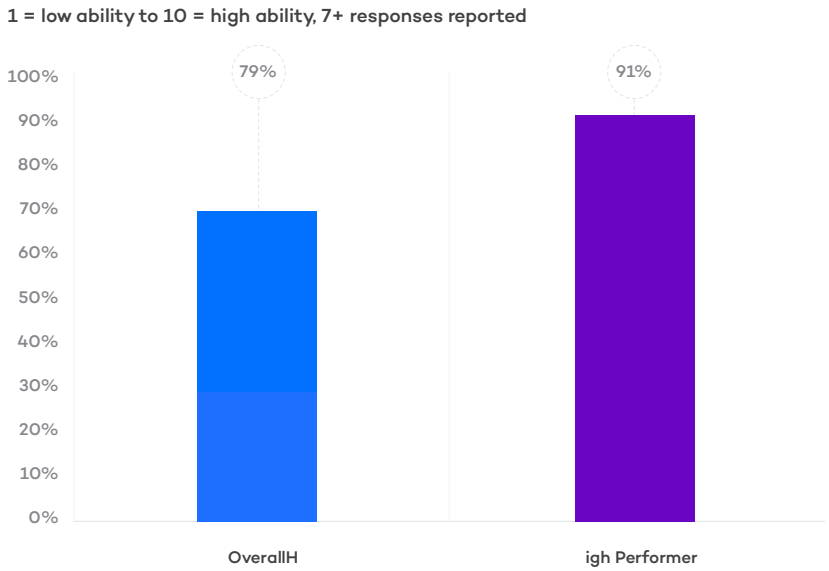


Figure 11. Ponemon Institute: relación entre ciber-resiliencia y la necesidad de disponer de recursos altamente cualificados y especializados y dedicados en ciber seguridad

Gobierno corporativo ciber-resiliente:

Los directivos de las empresas con alta ciber-resiliencia, son sensibles a la relación positiva que existe entre esta y el crecimiento económico, de marca y reputación de la organización.

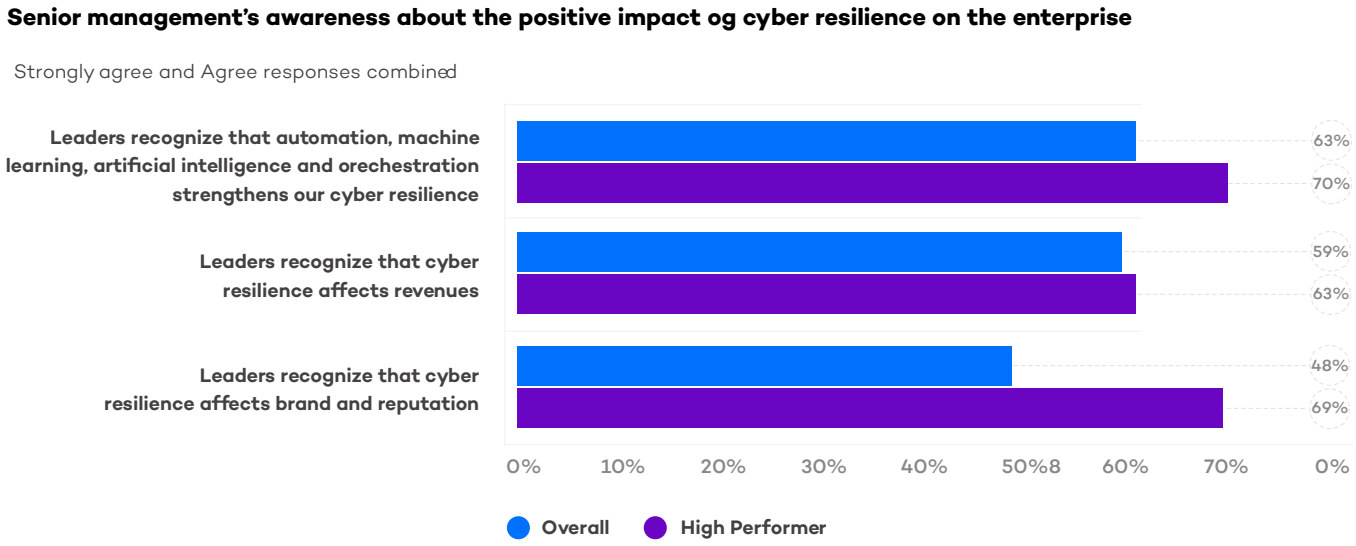


Figure 12. Ponemon Institute: La importancia de la involucración de la dirección en construir un alto nivel de ciber-resiliencia en sus empresas.

Conclusiones

La transformación digital que se está produciendo en casi todos los aspectos de nuestras vidas tiene una especial importancia cuando el concepto que evoluciona son las empresas, organizaciones y entes públicos, los dispositivos interconectados, las aplicaciones, herramientas y procesos productivos.

Desde un punto competitivo, la búsqueda de la optimización gracias a la transformación y aparición de nuevos instrumentos, medios, capacidades y procesos, es el origen de casi todas las iniciativas tanto en el ámbito privado como público.

Sin embargo, hay otro aspecto que no podemos dejar de lado en el camino hacia la transformación digital: la transformación debe ser también profunda en la ciberseguridad y gestión del riesgo empresarial.

Más aun conociendo la evolución en número y sofisticación de las amenazas. El cibercrimen es un negocio atractivo y muy lucrativo. Los atacantes cuentan cada vez con más y mejores recursos –tanto técnicos como económicos- lo que les permite desarrollar ataques cada vez más sofisticados. Todo esto resulta en amenazas más complejas y dinámicas, además de una mayor cantidad de ataques.

Equifax, CCleaner, WPA2, Vault7, CIA, KRACK, NSA, **WannaCry**, **Goldeneye/NotPetya,** Meltdown/ Spectre, **hackeo de elecciones**... Son algunos de los protagonistas muy recientes de infecciones masivas, robos o fugas de datos personales, ataques de ransomware, aplicaciones hackeadas para lanzar ataques contra un país, para llevar a cabo ataques dirigidos contra grandes empresas concretas, hasta vulnerabilidades que afectan a miles de millones de dispositivos.

Con casos reales como estos, no es de extrañar que el 75% de las empresas (según una reciente encuesta de McKinsey) considere que la ciberseguridad es una prioridad para el correcto desarrollo de su actividad. La situación de estrés descrita anteriormente, requiere de una reacción que suponga un nuevo enfoque en el programa de seguridad en toda la organización, que desarrollo y potencie una postura empresarial de ciber-resiliencia.

La ciber-resiliencia es la capacidad de una organización de mantener su propósito principal e integridad frente a la amenaza latente de los ataques de ciberseguridad.

Una empresa **ciber-resiliente** es aquella que puede prevenir, detectar, contener y recuperarse, minimizando el tiempo de exposición y el impacto en el negocio de innumerables amenazas graves contra datos, información y aplicaciones e infraestructura de IT. Especialmente contra los equipos, donde residen los activos más valiosos para la organización, ya que alcanzarlos supone también atacar la integridad de las identidades y usuarios.

El nuevo enfoque en el programa de seguridad, que lleve a la organización a ser ciber-resiliente, debe cubrir al menos los siguientes aspectos:

1. **Gestionar la ciberseguridad como un problema de gestión del riesgo corporativo**, no como un problema de IT y **adoptar una la dinámica del "ciclo de resiliencia".** Los elementos clave del ciclo de ciber-resiliencia incluyen:

    1. Priorizar los activos más valiosos de la organización.

    2. Priorizar, conocer y entender a los adversarios.Conocer e implantas las mejores defensas preventivas.

    3. Estar preparado para cuando los adversarios pueda sobre pasar todas las tecnologías de seguridad y detectarlos, contenerlos y remediar sus acciones lo antes posibles para minimizar el daño corporativo.

    4. Adoptar una postura de crisis continua buscando activamente amenazas.

5. Gestionar a nivel corporativo la comunicación de la situación de violación.

6. Definir y ejecutar constantemente iniciativas que reduzcan la superficie de ataque y así volver a empezar con el ciclo de mejora continua en la gestión de la seguridad corporativa.

2. **Fortalecer 4 pilares claves: prevención, detección y búsqueda proactiva de amenazas (Threat Hunting), contención y respuesta y la reducción de la superficie de ataque.**

3. **Adaptarse continuamente a las nuevas técnicas y tácticas de los hackers y otros atacantes.** El ser resiliente implica que esa adaptación se ha de realizar en el mínimo intervalo de tiempo, a la máxima velocidad, incluso en tiempo real.

4. **Priorizar y mitigar los riegos a todos los niveles de la organización**. Las empresas deben aprovechar las herramientas, productos y servicios gestionados que automatizan estas funciones de perfilar, catalogar, monitorizar toda la actividad en sus activos (humanos, datos, infraestructura) y aprender de ellos de forma que los sistemas de seguridad sean predictivo y acelere la prevención y/o detección precoz de los adversarios reduciendo el nivel del riesgo organizativo sin incurrir en costes, sobre todo operativos, desproporcionados.

5. **Gestionar el ciberriesgo mediante un gobierno colaborativo integral.**

Panda Security Summit | The European Cybersecurity Hub

#PASS2018