



Evaluación de la madurez en materia de seguridad y buenas prácticas en organizaciones del sector

INTRODUCCIÓN

Dirigir una empresa en el siglo XXI se parece mucho a nadar entre tiburones. El peligro es evidente: los cibercriminales se vuelven más poderosos, organizados y colaborativos con cada día que pasa. Aun así, las organizaciones se ven obligadas a nadar en el océano de la transformación digital, lo cual se está convirtiendo en una inquietud vital para los CEO de hoy en día. Sin embargo, esto implica adentrarse todavía más en aguas infestadas de tiburones.

Las tecnologías de la transformación digital (Big Data/análisis de datos, computación en la nube, movilidad y social business) dejan a las aplicaciones corporativas fuera de la seguridad de los controles perimetrales existentes en los terminales y en la red. Para los profesionales de la seguridad, esto supone una pérdida de visibilidad y control. Ya no es solo que estemos nadando en aguas turbias, sino que la puerta de esa jaula a prueba de tiburones que antes solía protegernos se ha abierto ahora de par en par.

Evitar la transformación digital no es una opción. Tan solo hay que mirar ejemplos de empresas como Blockbusters y Borders, que no han sido capaces de adaptarse a la nueva realidad y ser conscientes de sus implicaciones. Más bien, es preciso un cambio radical tanto en el enfoque tecnológico como en la mentalidad estratégica. Este informe tiene como objetivo descubrir las buenas prácticas de las que hacen gala las empresas del sector que tienen un enfoque más maduro en materia de seguridad. A fin de poder nadar entre tiburones, y tal vez incluso ser capaz de devolver los ataques, es preciso adoptar una nueva perspectiva.

UTILIZACIÓN DE ESTE INFORME

Este informe pretende ayudarle a comprender las características y la progresión de la madurez en materia de seguridad. En él se identifican ejemplos de buenas prácticas que puede seguir para mejorar su madurez en el ámbito de seguridad. Asimismo, se destacan los aceleradores de la innovación que influyen de manera particularmente notable en el aumento de los niveles de madurez. Por último, se ofrecen recomendaciones sobre cómo mejorar la posición de su empresa con respecto al resto de organizaciones del mismo sector. Estas reflexiones provienen de una encuesta, realizada en el verano de 2016, a 500 altos ejecutivos del sector de la seguridad en Francia, Alemania, Italia, España y Reino Unido.

PERFIL DE MADUREZ DE LAS EMPRESAS DEL SECTOR

De acuerdo a nuestra encuesta a 500 altos ejecutivos del sector de la seguridad, IDC ha dividido el mercado en cinco categorías de madurez. De menos a más, las categorías son las siguientes:

- ad-hoc**
- oportunista**
- repetible**
- gestionada**
- optimizada**

Las empresas se distribuyen, como suele ser lo normal, en una clásica "curva de campana", como puede apreciarse en la Figura 1

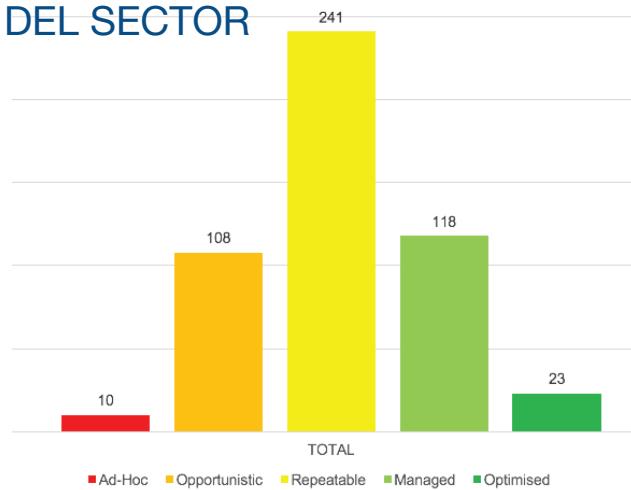


Figure 1

Fuente: IDC, 2016

En lo que respecta al enfoque sobre seguridad, hay muy pocas organizaciones de este sector que estén situadas en el extremo inferior, al igual que ocurre en el extremo superior. En cambio, la mayoría de empresas del sector se encuentran en un término medio. Si su empresa pretende nadar entre tiburones sin llevarse un escarmiento, debe aspirar a superar a las empresas de su mismo sector y adoptar buenas prácticas lo antes posible. La siguiente sección de este informe da una indicación de cuáles esas prácticas en materia de seguridad.

BUENAS PRÁCTICAS EN EL ÁMBITO DE LA SEGURIDAD

Tradicionalmente, el objetivo de la tecnología de seguridad ha sido el de proteger a las empresas frente a las amenazas conocidas. Al situar a los dispositivos, las aplicaciones y los datos detrás de la red de seguridad del cortafuego, los controles perimetrales existentes a nivel de dispositivo y red podían mantener a raya esas amenazas conocidas. Sin embargo, existen dos tendencias que están haciendo que estos modelos preventivos de seguridad sean insuficientes como enfoque independiente:

- Digital transformation is taking corporate applications and data beyond the perimeter, and outside the visibility and control of in-house security teams.
- La magnitud de las amenazas no tiene precedentes. Cada día aparecen más de un millón de nuevas variantes de software malicioso, y es sencillamente imposible generar firmas a un ritmo lo suficientemente rápido como para mantener las defensas tradicionales que tratan de bloquear nuevas amenazas.

Es evidente que hacen falta nuevos enfoques que ayuden a las empresas a identificar amenazas desconocidas y responder ante ellas, así como a bloquear las conocidas. La seguridad debe hacerse proactivamente y buscar indicadores potenciales de amenaza que se puedan corregir, en lugar de esperar a que un ataque se vuelva evidente. Sin embargo, para ello hace falta adoptar una nueva mentalidad en la estrategia de seguridad. En la Figura 2 puede apreciarse un análisis muy ilustrativo de los factores que se considera que limitan la eficacia de la seguridad en función de los niveles de madurez.

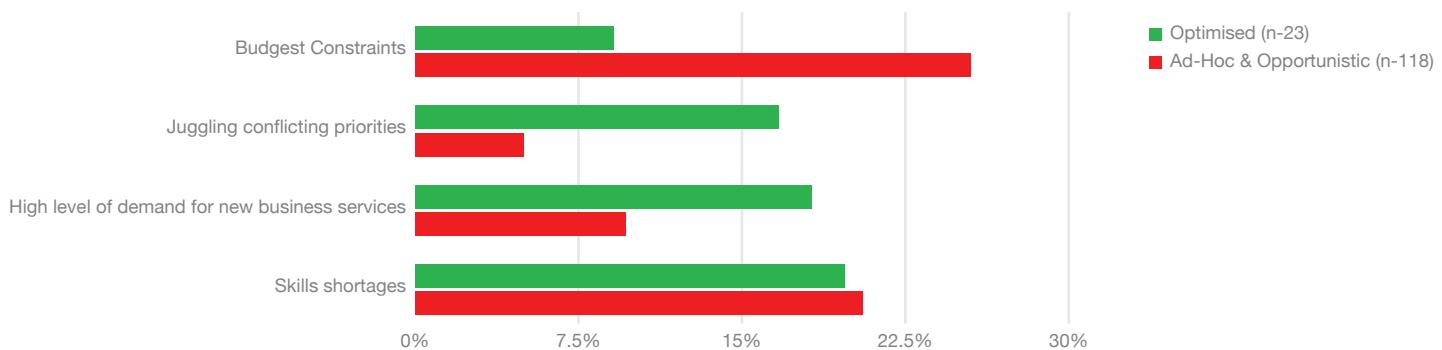


Figure 2

Fuente: IDC, 2016

Hay ciertos aspectos comunes que se aplican a todos los niveles de madurez. Concretamente, las principales limitaciones son el coste y la falta de talento. Esto no es ninguna sorpresa dada la escasez generalizada de talento que se da en el mercado de la seguridad. Sin embargo, es el grado de atención que se le preste al resto de preocupaciones lo que hace aflorar la comprensión sobre buenas prácticas.

En los niveles más bajos de madurez, las presiones en cuanto a costes y la falta de talento son las principales preocupaciones. Pero a niveles más altos, existe un mayor equilibrio entre estas áreas y cuestiones como la gestión de conflictos entre prioridades y el respaldo a la demanda de nuevos servicios comerciales. Esto pone de relieve un cambio drástico de mentalidad: en lo que respecta a la seguridad, una buena práctica es tener en cuenta las necesidades de la empresa.

Una vez asumido este cambio, las empresas deben valorar lo que ello significa desde el punto de vista de los enfoques en materia de seguridad práctica. En particular, es preciso alejarse de los modelos de seguridad reactiva y dirigirse hacia una seguridad proactiva. De hecho, como se muestra en la Figura 3, hay dos tendencias claras en función de las técnicas de madurez. Cuanto más madura es una empresa, es menos probable que no esté utilizando técnicas de seguridad proactivas, y es más probable que ya las esté planificando o utilizando.

Adopción de seguridad proactiva por nivel de madurez

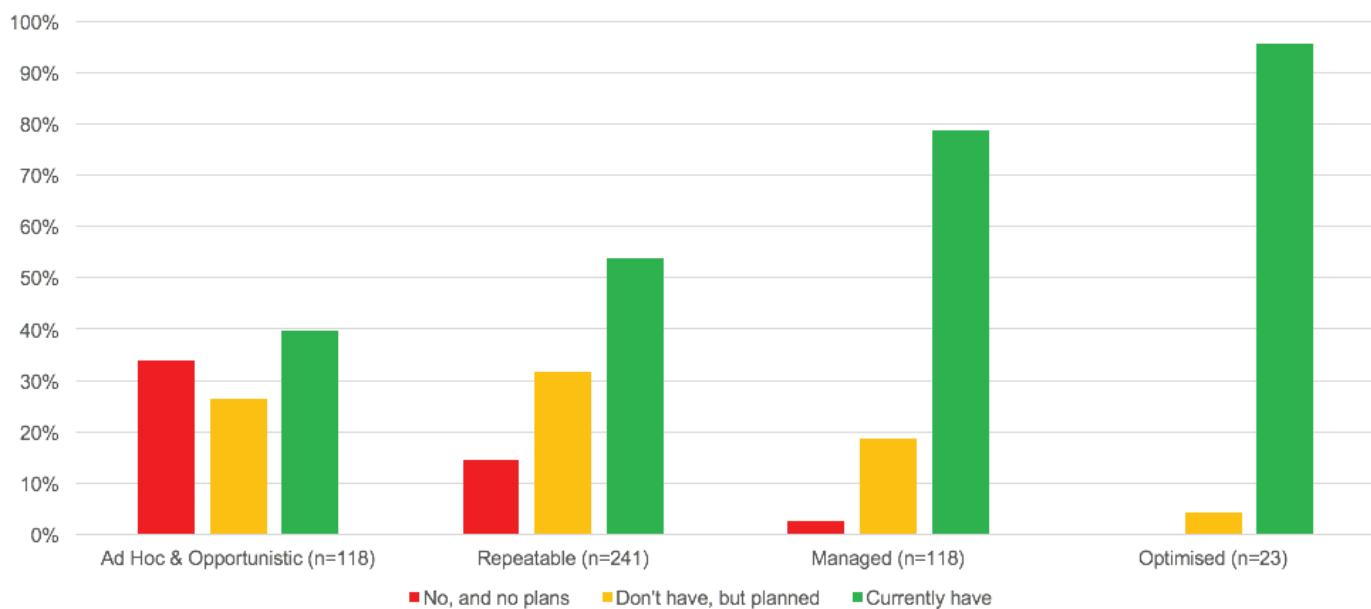


Figure 3

Fuente: IDC, 2016

Según nuestra encuesta, las principales tecnologías de seguridad que las empresas pueden adoptar para facilitar estos enfoques más proactivos son las siguientes: información sobre amenazas, inteligencia artificial y análisis heurístico del comportamiento del usuario. Como ocurre con las tecnologías proactivas, cuanto más maduro sea el enfoque de una empresa en cuestión de seguridad, más probable es que utilice soluciones como inteligencia artificial y análisis heurístico.

Aunque los enfoques proactivos sobre seguridad suponen una oportunidad para avanzar en la escala de madurez en materia de seguridad, también traen consigo sus propios desafíos. Por ejemplo, las técnicas proactivas requieren de la recopilación y supervisión de registros operacionales y de comportamiento en una escala mucho mayor. Dadas la presión a la que están sometidos los equipos de seguridad en lo que respecta a los recursos financieros, es preciso llevar a cabo un profundo análisis de las técnicas que contribuyan a aliviar las tensiones sobre los recursos internos. Las buenas prácticas muestran dos opciones posibles.

OUTSOURCING

Aunque la seguridad empresarial es compleja, la tónica general es mantener el control de la misma a nivel interno. Hay una serie de factores que contribuyen a ello. Para empezar, se considera que la seguridad es una actividad vital y cualquier externalización amenaza con reducir la visibilidad y el control que los equipos internos mantienen con respecto a la seguridad. Los proveedores de servicios de seguridad gestionados (PSSG) han hecho grandes promesas en el pasado, pero estas no siempre se han hecho realidad. Por último, los equipos internos pueden llegar a considerar el recurrir a tercera empresas como una admisión del fracaso y la constatación de que no son capaces de hacer el trabajo por sí solos.

Sin embargo, en un mundo interconectado, ninguna empresa por sí sola puede hacer frente a las amenazas. Esto es especialmente cierto cuando las empresas europeas poseen limitados recursos en cuestión de seguridad, y además existen otras empresas que cada vez están mejor posicionadas para prestar asistencia gracias a, por ejemplo, sus negocios a escala mundial, sus modelos de suministro industrializados y un mejor acceso a personal cualificado. Por lo tanto, para aquellas empresas que aspiran a adoptar buenas prácticas en materia de seguridad, los SSG son un factor importante a tener en cuenta.

Aunque los SSG pueden ser una herramienta útil para aliviar la presión a la que se someten los recursos internos, no puede ser la única respuesta. Un estudio de IDC indica que, en lugar de recurrir al outsourcing integral, la mejor opción reside en encontrar un equilibrio entre la prestación de servicios interna y los SSG, de modo que se atiendan tanto los objetivos empresariales como la disposición de la empresa al riesgo. Preservar las capacidades internas de las operaciones en materia de seguridad es importante para entender el impacto estratégico de las decisiones empresariales en cuestiones de seguridad, y viceversa. Dado que la seguridad está cada vez más orientada a la gestión de riesgos y constituye una preocupación que afecta a la organización en su conjunto, esta es una característica fundamental de las buenas prácticas en el ámbito de la gestión empresarial, cuanto más de las prácticas de seguridad.

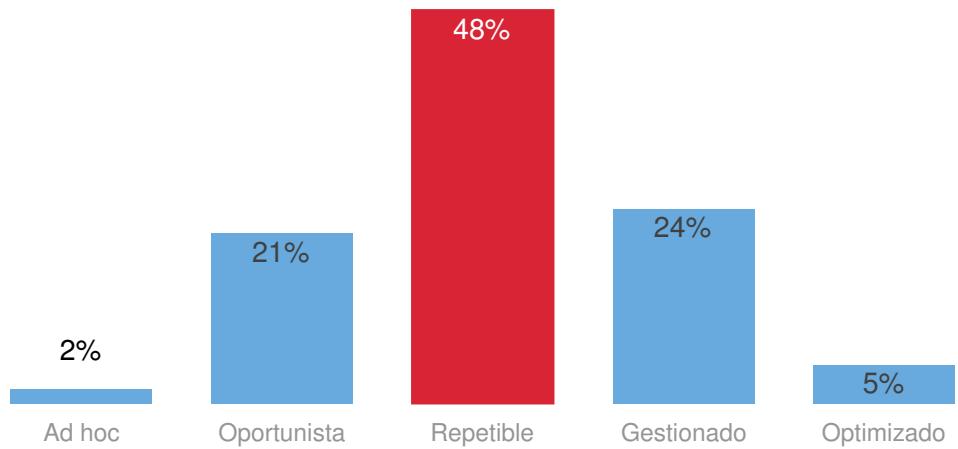
AUTOMATIZACIÓN

Además de los SSG, otro instrumento clave para que las empresas puedan afrontar la presión sobre los recursos y el desequilibrio entre la transformación digital y el panorama cambiante de las amenazas es la automatización. La automatización hace posible que se pueda llevar a cabo la gestión, e incluso la ejecución, de las operaciones de seguridad mediante productos de tecnología. La participación del personal interno ayuda a mantener la visibilidad y el control sobre la seguridad.

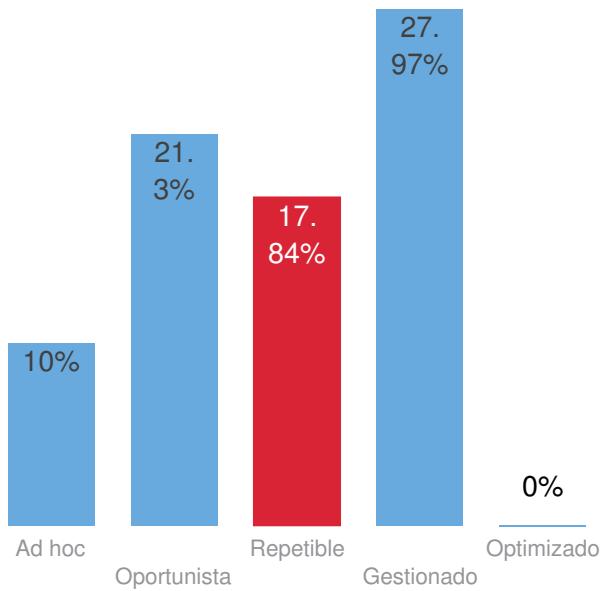
Esto tendrá consecuencias para la aparición de la inteligencia artificial y la computación cognitiva en el ámbito de la seguridad, que tiene como objetivo ceder la toma de decisiones a las máquinas para aliviar aún más la presión sobre los recursos. Sin embargo, está claro que las buenas prácticas (al menos por el momento) supondrán mantener un cierto grado de supervisión humana para asegurar el buen funcionamiento de las máquinas, o evitar que las decisiones más críticas las tomen robots.

CUSTOM REPORT SUMMARY AND OVERALL PERFORMANCE RANKING

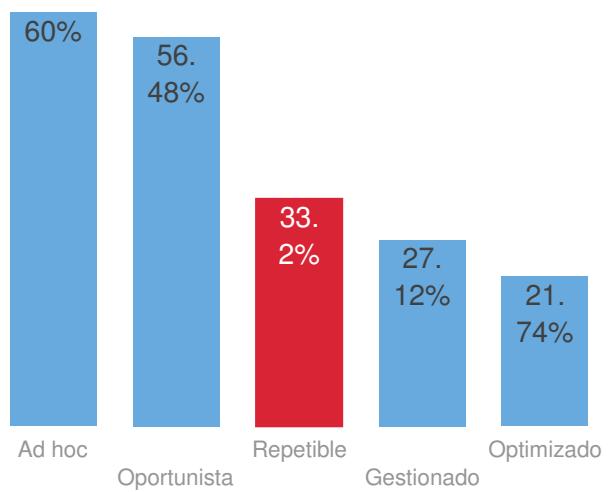
How you compare overall



Your comparison to others in your country



Your comparison to companies of similar size





PERFORMANCE RANKING BY CATEGORY

Cyber Risk Management and the Business



Clasificación: **REPETIBLE**

¡Cuidado! Está por detrás en este área clave de la gestión de los riesgos informáticos y necesita mejorar urgentemente la situación para reducir su exposición a amenazas informáticas y a posibles multas o daños a su reputación.

Cyber Risk Management Operations and Defence



Clasificación: **REPETIBLE**

¡Muy buen trabajo! Está al mismo nivel en esta área clave de gestión de riesgos informáticos, pero sigue siendo conveniente que busque nuevas formas de mejorar su preparación global frente a riesgos informáticos.

Cyber Risk Management Breach Detection and Remediation



Clasificación: **REPETIBLE**

¡Fantástico! Está por delante de sus colegas en lo que respecta a la gestión de riesgos informáticos conjuntamente con la empresa. Lo está haciendo muy bien en esta área de la gestión de los riesgos informáticos, pero no debe dormirse en los laureles ni dejar nunca de reevaluar sus actividades.

CYBER RISK MANAGEMENT AND THE BUSINESS PERFORMANCE RANKING BY QUESTION

Ahora vamos a ver cómo fue su desempeño en tres áreas clave de preparación frente a riesgos informáticos. En cada caso, veremos cuáles fueron sus resultados en comparación con otros con el mismo grado de preparación Repetible que usted. Para ello, comprobaremos si usted se encuentra por detrás, al mismo nivel o por delante de su colegas.

Si está al mismo nivel, puede compararse en términos generales con la mayoría de empresas con su mismo grado de preparación. Si está por delante, lo está haciendo bien en esta área y debe buscar otras áreas en las que deba mejorar para conseguir un enfoque equilibrado. Si está por detrás, debe dedicar atención y esfuerzos a este área para incrementar su grado de preparación frente a riesgos informáticos.

Si obtiene una calificación de al mismo nivel o adelantado en todas las secciones, está preparado para subir un nivel de preparación a corto plazo.

— Q1: ¿Cuál suele ser la opinión de la alta dirección de la empresa acerca del papel de las TI? Elija una

A: **Un facilitador de la eficiencia empresarial**

When compared with the next level, **Gestionado** you would be positioned as **Al mismo nivel**
idcs-cyber-risk-assessment.questions.q1.Al mismo nivel

— Q2: Cuando se trata de solicitudes empresariales de aplicaciones o servicios nuevos o mejorados, ¿qué afirmación refleja mejor las capacidades de su departamento de TI? Elija una

A: **En general no tenemos problemas con las solicitudes relativas a aplicaciones o servicios existentes, pero las solicitudes de servicios nuevos o mejorados nos plantean problemas.**

When compared with the next level, **Gestionado** you would be positioned as **Rezagado**
idcs-cyber-risk-assessment.questions.q2.Al mismo nivel

— Q3: ¿Qué afirmación describe mejor su actitud frente al riesgo a nivel empresarial? Elija una

A: **Tenemos tendencia a evitar riesgos, pero corremos algunos riesgos si hay una justificación muy buena.**

When compared with the next level, **Gestionado** you would be positioned as **Rezagado**
idcs-cyber-risk-assessment.questions.q3.Rezagado

— Q4: ¿Cuál de las siguientes opciones tienen ya implantadas para proteger su empresa si se produce un incidente? (1-Lo tenemos actualmente, 2-No lo tenemos, pero está previsto implantarlo, 3-No, y no prevemos implantarlo)

A:

Una evaluación formal de riesgos

No lo tenemos, pero está previsto implantarlo

Plan de comunicaciones internas

Lo tenemos actualmente

Plan de medidas correctivas de fallos de seguridad

Lo tenemos actualmente

Detección proactiva

No lo tenemos, pero está previsto implantarlo

Plan de comunicaciones externas y relaciones públicas

Lo tenemos actualmente

Seguro de riesgos informáticos

Lo tenemos actualmente

Plan de respuesta

Lo tenemos actualmente

Plan de notificación de fallos de seguridad

Lo tenemos actualmente

When compared with the next level, **stage4** you would be positioned as **Ahead**

Su modo de gestionar el riesgo de fallos de seguridad y planificar sus respuestas en caso de fallo de seguridad es muy previsor. Sin embargo, como siguiente paso, piense en cómo se podría aprovechar un seguro de riesgos informáticos no solo para reducir los costes de un posible fallo de seguridad, sino también como motor para la excelencia, lo que podría convertir la forma de gestionar los datos de los clientes en una ventaja competitiva.

— Q5: ¿Qué afirmación describe mejor cómo se maneja en su empresa la gestión de riesgos informáticos? Elija una

A: **No tiene un responsable específico.**

When compared with the next level, **Gestionado** you would be positioned as **Rezagado**
idcs-cyber-risk-assessment.questions.q5.Rezagado

— Q6: ¿Con cuál de las siguientes opciones cuentan ustedes como parte de su marco de trabajo en la gestión de riesgos informáticos? (Seleccione todas las que correspondan) [Sí/No]

A:

CEO (Director Ejecutivo)
No

CFO (Responsable de finanzas)
No

COO (Responsable de operaciones)
No

Miembro no ejecutivo de nivel de la junta centrado en riesgos/cumplimiento de la normativa/seguridad
Si

Miembro ejecutivo de nivel de la junta centrado en riesgos/cumplimiento de la normativa/seguridad
Si

Cargo específico de riesgos/cumplimiento de la normativa/seguridad (que no es miembro de la junta directiva)
Si

When compared with the next level, **stage4** you would be positioned as **Behind**

Las buenas prácticas en gestión de riesgos informáticos conllevan un alto grado de implicación de la alta dirección, así como contar con responsables de riesgos y cumplimiento especializados. Busque vías para lograr un mayor grado de implicación y responsabilidad de la empresa, sobre todo en lo que respecta a los expertos en cumplimiento y que haga partícipes a los jefes de operaciones. Haga un uso eficaz de terceros para evaluar las buenas prácticas.

— Q7: ¿En qué etapa, por lo general, participa TI en los proyectos e iniciativas empresariales? Seleccione solo una

A: **Desde el comienzo de la planificación**

When compared with the next level, **Gestionado** you would be positioned as **Adelantado**
idcs-cyber-risk-assessment.questions.q7.Adelantado

— Q8: ¿Cómo describiría el nivel de inversión de su organización en seguridad de TI? Seleccione solo una

A: **Ajustado, apenas cubre las operaciones esenciales**

When compared with the next level, **Gestionado** you would be positioned as **Rezagado**
idcs-cyber-risk-assessment.questions.q8.Rezagado

CYBER RISK MANAGEMENT OPERATIONS AND DEFENCE PERFORMANCE RANKING BY QUESTION

Ahora vamos a ver cómo fue su desempeño en tres áreas clave de preparación frente a riesgos informáticos. En cada caso, veremos cuáles fueron sus resultados en comparación con otros con el mismo grado de preparación Repetible que usted. Para ello, comprobaremos si usted se encuentra por detrás, al mismo nivel o por delante de su colegas.

Si está al mismo nivel, puede compararse en términos generales con la mayoría de empresas con su mismo grado de preparación. Si está por delante, lo está haciendo bien en esta área y debe buscar otras áreas en las que deba mejorar para conseguir un enfoque equilibrado. Si está por detrás, debe dedicar atención y esfuerzos a este área para incrementar su grado de preparación frente a riesgos informáticos.

Si obtiene una calificación de al mismo nivel o adelantado en todas las secciones, está preparado para subir un nivel de preparación a corto plazo.

 Q9: ¿En qué medida tienen ustedes implantadas las siguientes opciones para gestionar la seguridad física de sus TI? (1-Nada en absoluto, 5-Muy extensamente)

A:

- | | | |
|---|--|---|
| <input type="checkbox"/> Investigación de los antecedentes del personal de seguridad
5 | <input type="checkbox"/> Citas concertadas previamente
5 | <input type="checkbox"/> Verificación de la identidad
1 |
| <input type="checkbox"/> Controles de entrada y de salida
1 | <input type="checkbox"/> Autenticación biométrica
1 | <input type="checkbox"/> Supervisión por circuito cerrado de televisión
1 |
| <input type="checkbox"/> Acompañamiento (el personal y los visitantes deben trabajar en parejas o ir acompañados)
1 | <input type="checkbox"/> Cambio de autorización, aprobación y registro
1 | |

When compared with the next level, stage4 you would be positioned as **Behind**

Considere la posibilidad de hacer un uso más amplio de estas técnicas, así como de algunas técnicas de segunda generación (por ejemplo, Investigación de los antecedentes del personal de seguridad, acompañamiento).

 Q10: ¿Cuál de las siguientes opciones describe mejor su adopción y aplicación de buenas prácticas de seguridad de las TI? Elija una

A: **No lo hacemos.**

When compared with the next level, **Gestionado** you would be positioned as **Rezagado**
idcs-cyber-risk-assessment.questions.q10.Rezagado

 Q11: ¿En qué medida están ustedes preparados para los siguientes aspectos de la evaluación y aplicación en su organización del cumplimiento de la norma GDPR (Reglamento General sobre la Protección de Datos)? (1-No estamos preparados, 5-Estamos muy bien preparados)

A:

<input type="checkbox"/> Conocimiento de las obligaciones	<input type="checkbox"/> Evaluación de las capacidades y carencias	<input type="checkbox"/> Planificación de la implantación
	1	1
<input type="checkbox"/> Ejecución de la implantación	<input type="checkbox"/> Mejora continua/buenas prácticas más allá de la propia GDPR (más allá de la normativa)	<input type="checkbox"/> Comprensión de la mitigación de las sanciones basada en la detección/correción tempranas
1	5	5

When compared with the next level, stage4 you would be positioned as **Behind**

Para progresar en la escala de madurez, adquiera una noción de las obligaciones que impondrá el RGPD, planifique la implementación de esas responsabilidades y luego lleve a cabo ese plan.

— Q12: ¿Tienden ustedes a invertir tácticamente (productos puntuales/según necesidades) o estratégicamente (como parte de un plan) en productos o soluciones de seguridad de TI? Elija una

A: **En general compramos tácticamente a medida que surgen problemas, pero hacemos algunas compras estratégicas.**

When compared with the next level, **Gestionado** you would be positioned as **Rezagado**

[idcs-cyber-risk-assessment.questions.q12.Rezagado](#)

— Q13: ¿Con qué frecuencia informan ustedes a la empresa sobre el estado de la seguridad de las TI?

Elija una

A: **Trimestralmente**

When compared with the next level, **Gestionado** you would be positioned as **Al mismo nivel**

[idcs-cyber-risk-assessment.questions.q13.Al mismo nivel](#)

— Q14: ¿Cuál es su principal medio para gestionar su infraestructura de seguridad de las TI? Elija solo una

A: **Utilizamos principalmente herramientas especializadas de gestión de la seguridad.**

When compared with the next level, **Gestionado** you would be positioned as **Al mismo nivel**

[idcs-cyber-risk-assessment.questions.q14.Al mismo nivel](#)

— Q15: "¿En qué medida han adoptado ustedes la automatización en su gestión de la seguridad de las TI? Elija solo una

A: **Automatización en todos los ámbitos**

When compared with the next level, **Gestionado** you would be positioned as **Adelantado**

[idcs-cyber-risk-assessment.questions.q15.Adelantado](#)

— Q16: Cuando se trata de su uso de la automatización, ¿cómo piensan cambiar el uso que hacen de la misma?

A: **Dejarla igual**

When compared with the next level, **Gestionado** you would be positioned as **Al mismo nivel**

[idcs-cyber-risk-assessment.questions.q16.Al mismo nivel](#)

 Q17: ¿Utilizan ustedes las siguientes opciones con respecto a la seguridad de las TI – defensa? Sí/No

A:

- | | | |
|--|---|---|
| <input type="checkbox"/> NGFW (cortafuegos de próxima generación)
No | <input type="checkbox"/> IPS/IDS (detección de intrusiones/protección contra intrusiones)
No | <input type="checkbox"/> Administración de vulnerabilidades
No |
| <input type="checkbox"/> Micro segmentación (separación y aislamiento detallados del tráfico entre servidores o dominios específicos)
No | <input type="checkbox"/> Gestión unificada de la seguridad (intercambio de datos e información entre dispositivos y herramientas),
No | <input type="checkbox"/> Servicio profesional de seguridad de terceros (venta/diseño/implantación)
No |

When compared with the next level, stage4 you would be positioned as **Behind**

Los más avanzados en gestión de riesgos informáticos utilizan masivamente una serie de productos de seguridad a su disposición para ofrecer protección en toda la red corporativa. Trabajar con especialistas de servicios profesionales de seguridad externos para que le ayuden a diseñar e implementar enfoques apropiados también puede permitirle dedicar menos tiempo a tareas de implementación y mejorar las capacidades.

Q25: ¿Qué enunciado describe mejor la extensión de su uso de proveedores de servicios gestionados de seguridad? Seleccione solo una

A: **Los utilizamos de una manera limitada, pero preferimos hacer las cosas internamente.**

When compared with the next level, Gestionado you would be positioned as Rezagado
idcs-cyber-risk-assessment.questions.q25.Rezagado

CYBER RISK MANAGEMENT BREACH DETECTION AND REMEDIATION PERFORMANCE RANKING BY QUESTION

Ahora vamos a ver cómo fue su desempeño en tres áreas clave de preparación frente a riesgos informáticos. En cada caso, veremos cuáles fueron sus resultados en comparación con otros con el mismo grado de preparación Repetible que usted. Para ello, comprobaremos si usted se encuentra por detrás, al mismo nivel o por delante de su colegas.

Si está al mismo nivel, puede compararse en términos generales con la mayoría de empresas con su mismo grado de preparación. Si está por delante, lo está haciendo bien en esta área y debe buscar otras áreas en las que deba mejorar para conseguir un enfoque equilibrado. Si está por detrás, debe dedicar atención y esfuerzos a este área para incrementar su grado de preparación frente a riesgos informáticos.

Si obtiene una calificación de al mismo nivel o adelantado en todas las secciones, está preparado para subir un nivel de preparación a corto plazo.

— Q18: ¿Utilizan ustedes las siguientes opciones con respecto a la seguridad de las TI – detección de fallos en la seguridad? Sí/No

A:

- | | | |
|---|---|--|
| <input type="checkbox"/> Servicios de inteligencia de amenazas
No | <input type="checkbox"/> Análisis en tiempo real
No | <input type="checkbox"/> Protección avanzada contra amenazas/entorno controlado
No |
| <input type="checkbox"/> IA/heurística
No | <input type="checkbox"/> Escaneo de malware
No | |

When compared with the next level, stage4 you would be positioned as **Behind**
idcs-cyber-risk-assessment.questions.q18.Rezagado

— Q19: "¿Utilizan ustedes las siguientes opciones con respecto a la seguridad de las TI – respuesta a fallos de seguridad? Sí/No

A:

- | | | |
|---|--|---|
| <input type="checkbox"/> Honeypot (sistema de señuelos) / Recogida de inteligencia
Si | <input type="checkbox"/> Monitor de procesos de registro y análisis
Si | <input type="checkbox"/> Recuperación de fallos/recuperación del sistema
Si |
| <input type="checkbox"/> Equipos tigre/adelante (Tiger/go)
Si | <input type="checkbox"/> Socio externo de respuesta a incidentes
Si | |

When compared with the next level, stage4 you would be positioned as **Ahead**
idcs-cyber-risk-assessment.questions.q19.Rezagado

— Q20: "¿Utilizan ustedes las siguientes opciones con respecto a la seguridad de TI – medidas correctivas de fallos en la seguridad? (Sí/No)

A:

- | | | |
|---|--|---|
| <input type="checkbox"/> Corrección automatizada (basada en el aprendizaje automático)
Si | <input type="checkbox"/> Actualizaciones de la política
Si | <input type="checkbox"/> Política de recuperación ante desastres
Si |
| <input type="checkbox"/> Proveedores externos de recuperación ante desastres
Si | <input type="checkbox"/> Evaluaciones de compromiso
Si | |

When compared with the next level, stage4 you would be positioned as **Ahead**
idcs-cyber-risk-assessment.questions.q20.Rezagado

— Q21: ¿Han realizado las siguientes acciones respecto a su comprensión de su perfil de riesgo informático? Sí/No?

A:

- | | | |
|---|--|--|
| <input type="checkbox"/> Han evaluado el riesgo de sufrir un fallo de seguridad informática | <input type="checkbox"/> Comprenden la escala potencial de la exposición | <input type="checkbox"/> Han realizado una evaluación de datos de los datos críticos |
| Si | Si | Si |
| <input type="checkbox"/> Comprenden la postura de la cadena ampliada de suministro o socios | <input type="checkbox"/> Han desarrollado un plan de respuesta ante fallos en la seguridad | |
| Si | Si | |

When compared with the next level, stage4 you would be positioned as **Ahead**
idcs-cyber-risk-assessment.questions.q21.Rezagado

— Q23: ¿Con qué frecuencia ponen a prueba sus capacidades de defensa de la seguridad de TI mediante la verificación por parte de terceros? Seleccione solo una

A: **Cada 6 meses**

When compared with the next level, **Gestionado** you would be positioned as Rezagado
idcs-cyber-risk-assessment.questions.q23.Al mismo nivel

— Q24: ¿Con qué frecuencia ponen a prueba sus planes de respuesta a incidentes de fallos de seguridad informática? Seleccione solo una

A: **Nunca**

When compared with the next level, **Gestionado** you would be positioned as Rezagado
idcs-cyber-risk-assessment.questions.q24.Rezagado

TOLERANCIA AL CAMBIO

Uno de los últimos factores que hay que tener en cuenta a la hora de comprender el grado de aceptación de las empresas a la necesidad de “nadar entre tiburones” es su capacidad de adaptarse al cambio en el ámbito de las TI. Como se ha mencionado anteriormente en este informe, los criterios de buenas prácticas en materia de ciberseguridad suponen una variación con respecto a los comportamientos tradicionales que se han ido desarrollando a lo largo de décadas. Para poder modificar la mentalidad y la filosofía en el ámbito de la seguridad, es fundamental tener la capacidad de dar la bienvenida al cambio en las TI subyacentes.

Un ejemplo clave en este sentido es la transformación digital, una de las principales razones por las que las empresas se ven, de entrada, obligadas a adentrarse en aguas infestadas de tiburones. Es posible que la práctica habitual entre los profesionales de la seguridad sea la de tratar de impedir la adopción de nuevas tecnologías como social business, movilidad, Big Data/análisis de datos y la nube. Adoptarlas supone correr riesgos. No obstante, este no es el enfoque más maduro; en vez de poner trabas a la transformación digital, las empresas inteligentes deben tratar de alentar a sus usuarios, poniendo a su disposición las herramientas necesarias para adoptar la transformación digital de forma segura.

Como se indica en la Figura 4 a continuación, cuanto más madura es una organización según lo definido por el marco de este estudio, más cómoda se siente adaptándose a los cambios en las TI. En el otro extremo, las empresas menos maduras tienden a pasarlo mal con cualquier cambio en el ámbito de las TI o, cuando menos, tienen dificultades cuando se les pide que implementen otros cambios a las aplicaciones y servicios que no sean los mínimos. No obstante, a medida que vamos subiendo por la escala de madurez, va siendo más probable que la empresa se describa a sí misma como capacitada para adaptarse a dichos cambios o, incluso, "muy capacitada" para ello.

Estos hallazgos muestran que, en el contexto actual de la seguridad, una de las claves para ser una empresa exitosa y dinámica reside en adoptar un enfoque maduro sobre la seguridad y ser capaz de sacar partido a los cambios en las TI (en vez de tenerles miedo). La puerta se abre en ambas direcciones, siendo un asunto reflejo del otro. La capacidad de efectuar cambios en las TI requiere conocer en profundidad las posibles implicaciones en materia de seguridad. Al mismo tiempo, para adoptar una postura madura sobre seguridad, es fundamental tener la capacidad de implementar los cambios necesarios en las TI.

Capacidad de adaptarse al cambio según el nivel de madurez en el ámbito de la ciberseguridad

Q2. When it comes to business requests for new or enhanced applications or services, which statement best reflects your IT department's capabilities?

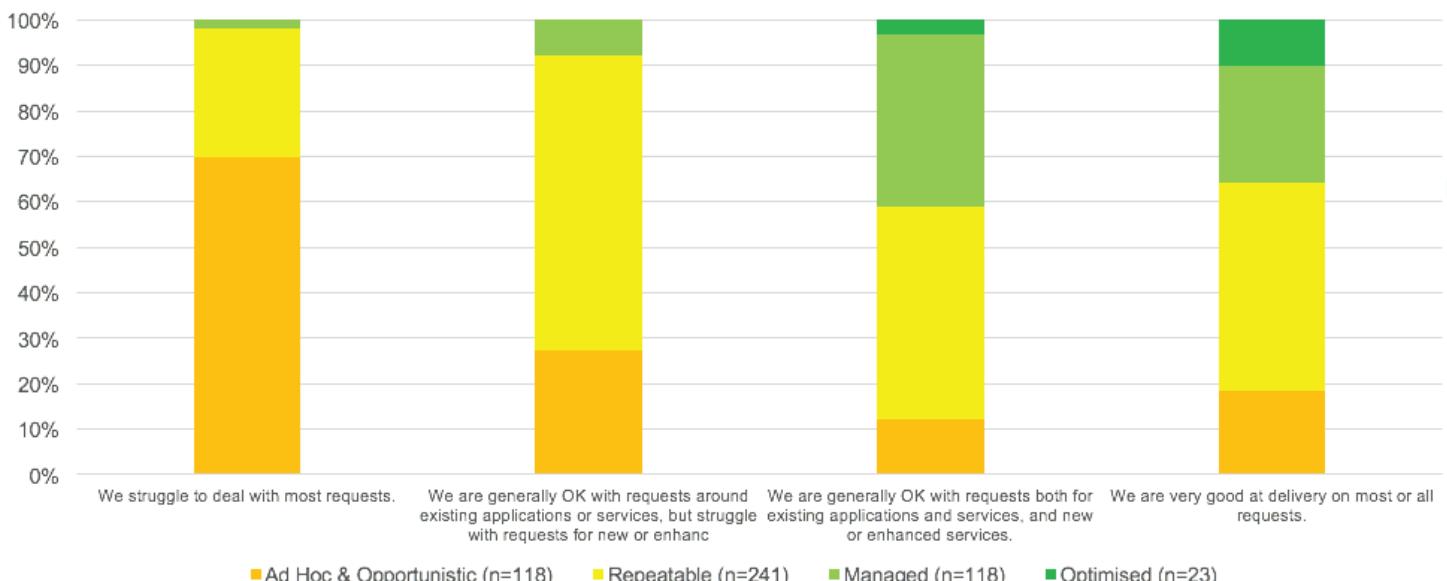


Figure 4 Fuente: IDC, 2016

10 RECOMENDACIONES PARA SU ORGANIZACIÓN

A continuación, se incluyen diez recomendaciones que proporcionan un marco para que su empresa mejore su nivel de madurez en el ámbito de la seguridad:

- **Compare su posición con la de empresas similares en términos de sector, tamaño y ubicación geográfica.**
- **Determine el grado de madurez de su empresa y hasta dónde está dispuesta a llegar.**
- **Determine las carencias de su enfoque actual en materia de seguridad comparándolo con el nivel al que desea llegar.**
- **Considere la posibilidad de recurrir a especialistas en seguridad externos para ayudarle a diseñar e implementar los cambios necesarios para alcanzar su objetivo.**
- **Identifique los procesos y actividades de seguridad que son vitales en comparación con aquellos que tienen poco valor y son repetitivos.**
- **Piense en qué áreas se podrían automatizar actividades de menor valor para reducir el uso de recursos.**
- **Investigue en qué casos se podría obtener una mejora de resultados trabajando con PSSG. Las actividades de menor valor pueden ser un buen punto de partida para aprovechar los modelos globales e industrializados de prestación de servicios.**
- **Sin embargo, a medida que los SSG van siendo cada vez más habituales en los negocios, piense en dónde podrían encontrarse recursos especializados que sean capaces de mejorar los resultados deseados, teniendo en cuenta no solo el coste sino también la calidad.**
- **Adopte un enfoque de seguridad basado en riesgos que abarque toda la empresa. Todos los usuarios constituyen una "amenaza interna" potencial, por lo que la cultura y la estrategia en materia de seguridad deben ser integrales.**
- **Haga partícipes a los responsables de seguridad de las nuevas iniciativas empresariales desde el principio. Si se asegura de que las nuevas iniciativas sean "seguras desde su diseño", se ahorrará problemas más adelante.**