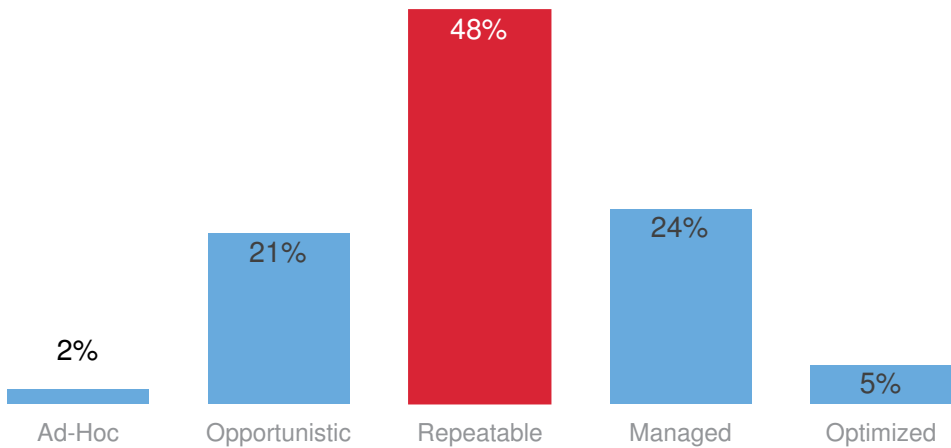


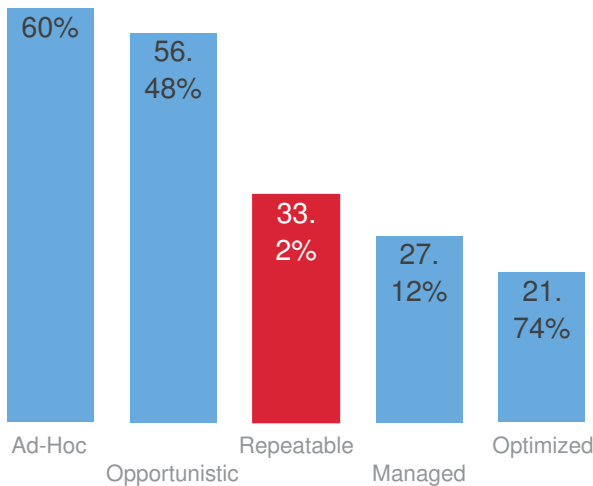
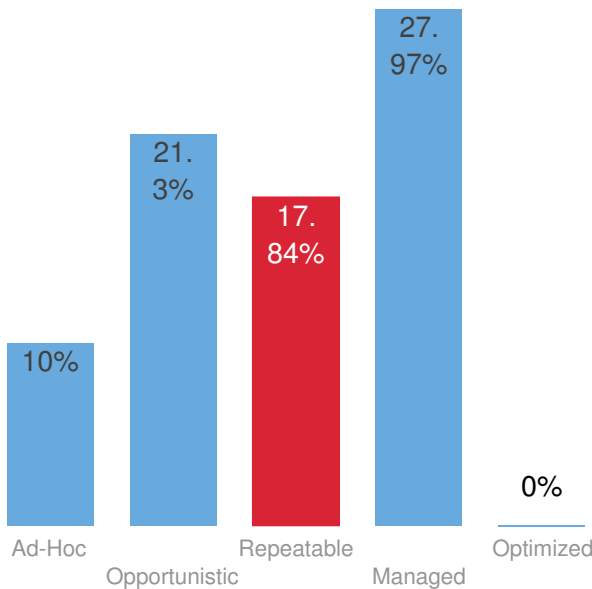
CUSTOM REPORT SUMMARY AND OVERALL PERFORMANCE RANKING

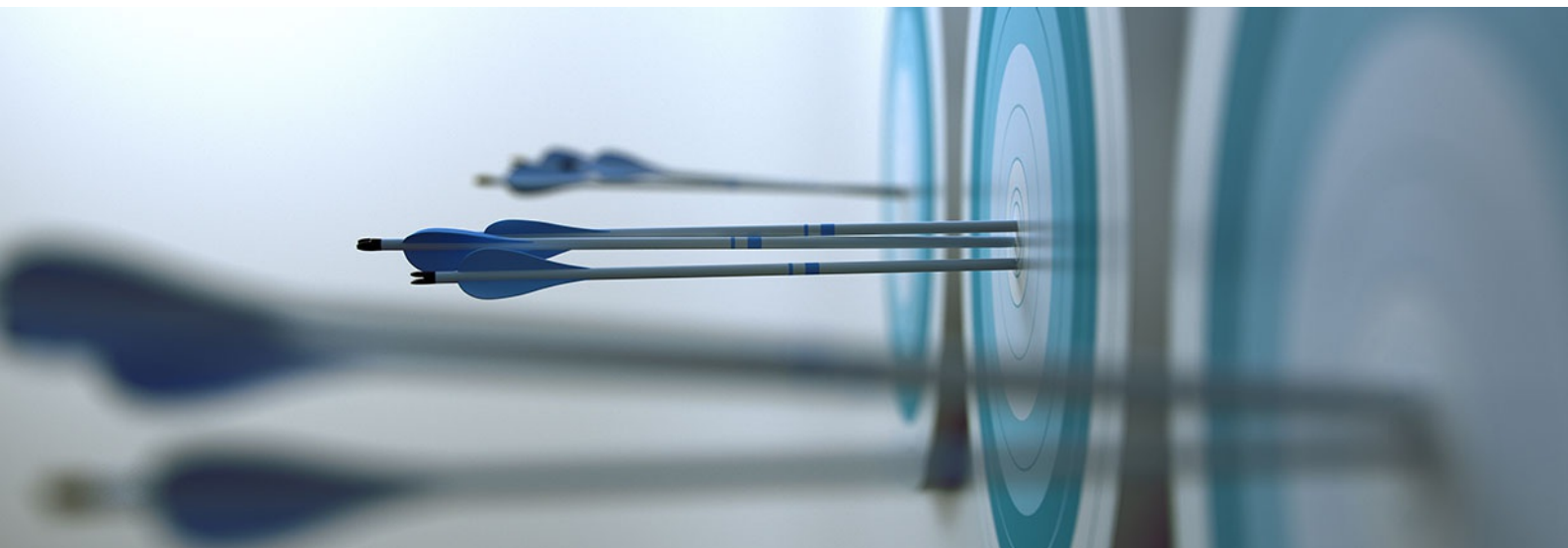
How you compare overall



Your comparison to others in your country

Your comparison to companies of similar size





PERFORMANCE RANKING BY CATEGORY

Cyber Risk Management and the Business



BEHIND

Ranking: **REPEATABLE**

Warning! You are behind in this core area of Cyber Risk management, and need to urgently improve matters to reduce your exposure to cyber threats and potential fines or loss of reputation.

Cyber Risk Management Operations and Defence



INLINE

Ranking: **REPEATABLE**

Job well done! You are performing in-line in this area of Cyber Risk management, but should still look to new approaches to help you improve your overall Cyber Risk readiness.

Cyber Risk Management Breach Detection and Remediation



AHEAD

Ranking: **REPEATABLE**

Top job! You are ahead of your peers when it comes to managing Cyber Risk in conjunction with the business. You are performing very well in this area of Cyber Risk management but should not become complacent and continually reassess what you do.

CYBER RISK MANAGEMENT AND THE BUSINESS PERFORMANCE RANKING BY QUESTION

We're now going to look at how you performed in three key areas of Cyber Risk Readiness. In each case, we'll look at how you compared to others in the same readiness ranking of **Repeatable** as yourself. To do this, we look at whether you are behind, in-line or ahead of your peers.

If you are in-line, you are broadly comparable to most companies at your level of readiness. If you are ahead, you are doing well in this area and should be looking at other areas to improve to get a balanced approach. If you are behind, you need to focus attention and investment in this area to bring your Cyber Risk Readiness in to line.

If you achieve a rating of in-line or ahead in all sections, you are ready to be moving up a readiness level in short order."

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, **Managed** 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, **Managed** 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, **Managed** 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

☐ Detección proactiva
No lo tenemos, pero está previsto implantarlo

☐ Plan de respuesta
Lo tenemos actualmente

☐ Plan de comunicaciones internas
Lo tenemos actualmente

☐ Plan de comunicaciones externas y relaciones públicas
Lo tenemos actualmente

☐ Plan de notificación de fallos de seguridad
Lo tenemos actualmente

☐ Plan de medidas correctivas de fallos de seguridad
Lo tenemos actualmente

☐ Seguro de riesgos informáticos
Lo tenemos actualmente

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

You are forward thinking in how you manage the risk of security breaches and plan your responses in the event of a breach. However, as a next step, consider how cyber risk insurance can be harnessed not only to mitigate the potential costs of a breach, but also as a driver for excellence - and thus it becomes a potential source of competitive advantage in how customer data is handled.

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, **Managed** 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**

Best practice in Cyber Risk management involves broad CxO engagement as well as having focused Risk and Compliance officers. Consider ways to bring more involvement and responsibility from the business, particularly with compliance experts and involving the operations leaders. Make effective use of third parties to gauge best practice.

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, **Managed** 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, **Managed** you would be positioned as **Rezagado**

idcs-cyber-risk-assessment.questions.q8.Rezagado

CYBER RISK MANAGEMENT OPERATIONS AND DEFENCE

PERFORMANCE RANKING BY QUESTION

We're now going to look at how you performed in three key areas of Cyber Risk Readiness. In each case, we'll look at how you compared to others in the same readiness ranking of **Repeatable** as yourself. To do this, we look at whether you are behind, in-line or ahead of your peers.

If you are in-line, you are broadly comparable to most companies at your level of readiness. If you are ahead, you are doing well in this area and should be looking at other areas to improve to get a balanced approach. If you are behind, you need to focus attention and investment in this area to bring your Cyber Risk Readiness in to line.

If you achieve a rating of in-line or ahead in all sections, you are ready to be moving up a readiness level in short order."

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:

☐ Investigación de los antecedentes del personal de seguridad
5

☐ Citas concertadas previamente
5

☐ Verificación de la identidad
1

☐ Controles de entrada y de salida
1

☐ Autenticación biométrica
1

☐ Supervisión por circuito cerrado de televisión
1

☐ Acompañamiento (el personal y los visitantes deben trabajar en parejas o ir acompañados)
1

☐ Cambio de autorización, aprobación y registro
1

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

Consider making more extensive use of these techniques, as well as some of the next-phase techniques (e.g. security staff screening, man-shadowing).

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, **Managed** 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:

☐ Conocimiento de las obligaciones
3

☐ Evaluación de las capacidades y carencias
1

☐ Planificación de la implantación
1

☐ Ejecución de la implantación
1

☐ Mejora continua/buenas prácticas más allá de la propia GDPR (más allá de la normativa)
5

☐ Comprensión de la mitigación de las sanciones basada en la detección/corrección tempranas
5

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

In order to move up the maturity scale, develop an understanding of the obligations that GDPR brings, plan for implementation of those responsibilities and then execute on that 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, **Managed** 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, **Managed** 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, **Managed** 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, **Managed** 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, **Managed** 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:

☐ NGFW (cortafuegos de próxima generación)

No

☐ IPS/IDS (detección de intrusiones/protección contra intrusiones)

No

☐ Administración de vulnerabilidades

No

☐ Micro segmentación (separación y aislamiento detallados del tráfico entre servidores o dominios específicos)

No


☐ Gestión unificada de la seguridad (intercambio de datos e información entre dispositivos y herramientas),


No

☐ Servicio profesional de seguridad de terceros (pre-venta/diseño/implantación)

No

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

The most advanced at Cyber Risk Mangement make extensive use of a range of security products that are available to offer protection across the corporate network. Working with third party professional security services specialists to help you design and implement appropriate approaches can also but time to implementation and boost capabilities.
-  **FireEye**

 **Hewlett Packard
Enterprise**

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, **Managed** you would be positioned as Rezagado

idcs-cyber-risk-assessment.questions.q25.Rezagado

CYBER RISK MANAGEMENT BREACH DETECTION AND REMEDIATION PERFORMANCE RANKING BY QUESTION

We're now going to look at how you performed in three key areas of Cyber Risk Readiness. In each case, we'll look at how you compared to others in the same readiness ranking of **Repeatable** as yourself. To do this, we look at whether you are behind, in-line or ahead of your peers.

If you are in-line, you are broadly comparable to most companies at your level of readiness. If you are ahead, you are doing well in this area and should be looking at other areas to improve to get a balanced approach. If you are behind, you need to focus attention and investment in this area to bring your Cyber Risk Readiness in to line.

If you achieve a rating of in-line or ahead in all sections, you are ready to be moving up a readiness level in short order."

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
Si | <input type="checkbox"/> Comprenden la escala potencial de la exposición
Si | <input type="checkbox"/> Han realizado una evaluación de datos de los datos críticos
Si |
| <input type="checkbox"/> Comprenden la postura de la cadena ampliada de suministro o socios
Si | <input type="checkbox"/> Han desarrollado un plan de respuesta ante fallos en la seguridad
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, **Managed** 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, **Managed** you would be positioned as Rezagado

idcs-cyber-risk-assessment.questions.q24.Rezagado