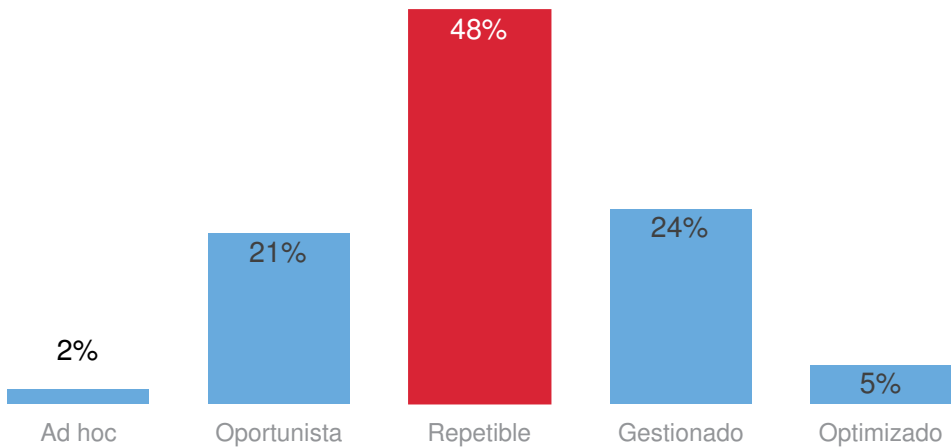


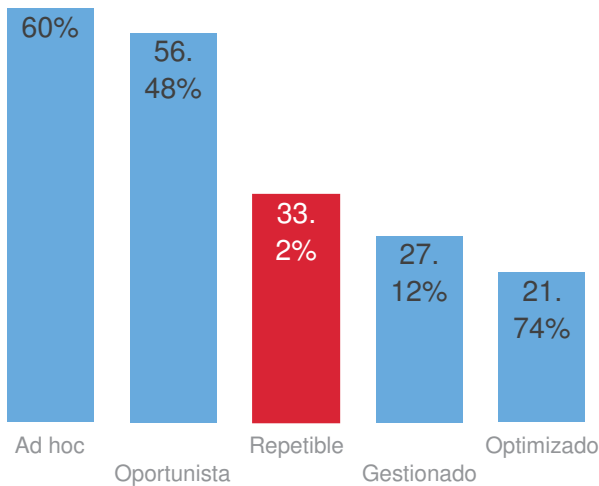
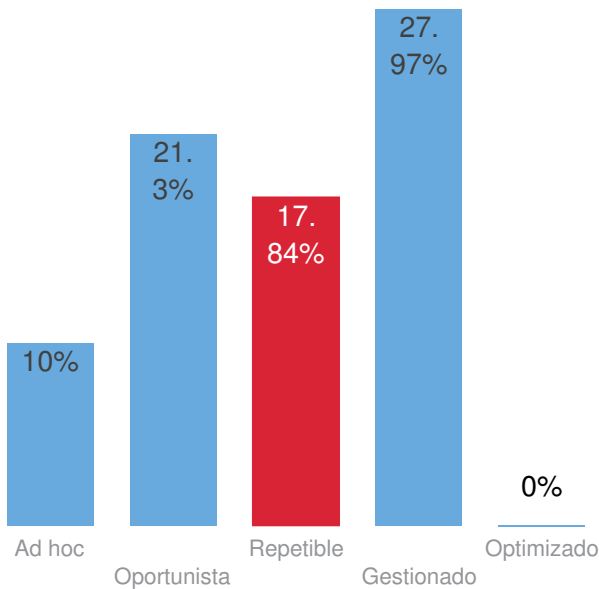
CUSTOM REPORT SUMMARY AND OVERALL PERFORMANCE RANKING

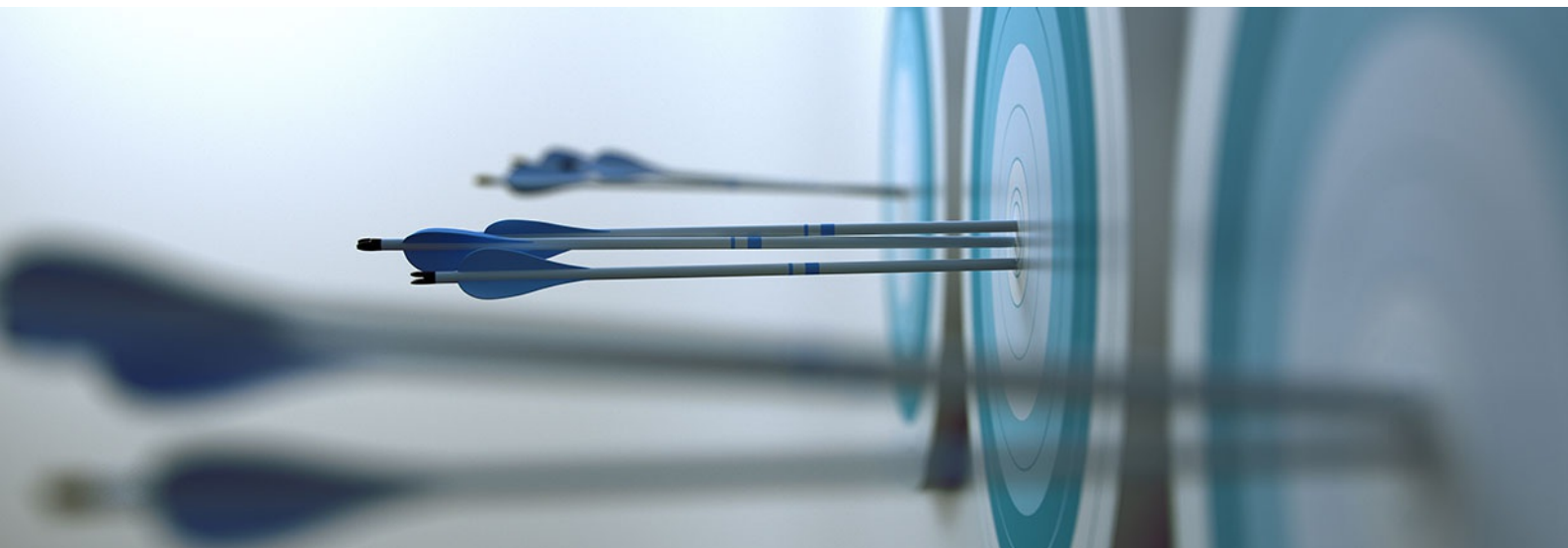
How you compare overall



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:

- | | | |
|---|---|---|
| <input type="checkbox"/> Una evaluación formal de riesgos
No lo tenemos, pero está previsto implantarlo | <input type="checkbox"/> Detección proactiva
No lo tenemos, pero está previsto implantarlo | <input type="checkbox"/> Plan de respuesta
Lo tenemos actualmente |
| <input type="checkbox"/> Plan de comunicaciones internas
Lo tenemos actualmente | <input type="checkbox"/> Plan de comunicaciones externas y relaciones públicas
Lo tenemos actualmente | <input type="checkbox"/> Plan de notificación de fallos de seguridad
Lo tenemos actualmente |
| <input type="checkbox"/> Plan de medidas correctivas de fallos de seguridad
Lo tenemos actualmente | <input type="checkbox"/> Seguro de riesgos informáticos
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:

☐ 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**

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
3 | <input type="checkbox"/> Evaluación de las capacidades y carencias
1 | <input type="checkbox"/> Planificación de la implantación
1 |
| <input type="checkbox"/> Ejecución de la implantación
1 | <input type="checkbox"/> Mejora continua/buenas prácticas más allá de la propia GDPR (más allá de la normativa)
5 | <input type="checkbox"/> 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**

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/segun 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 (pre-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
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, **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