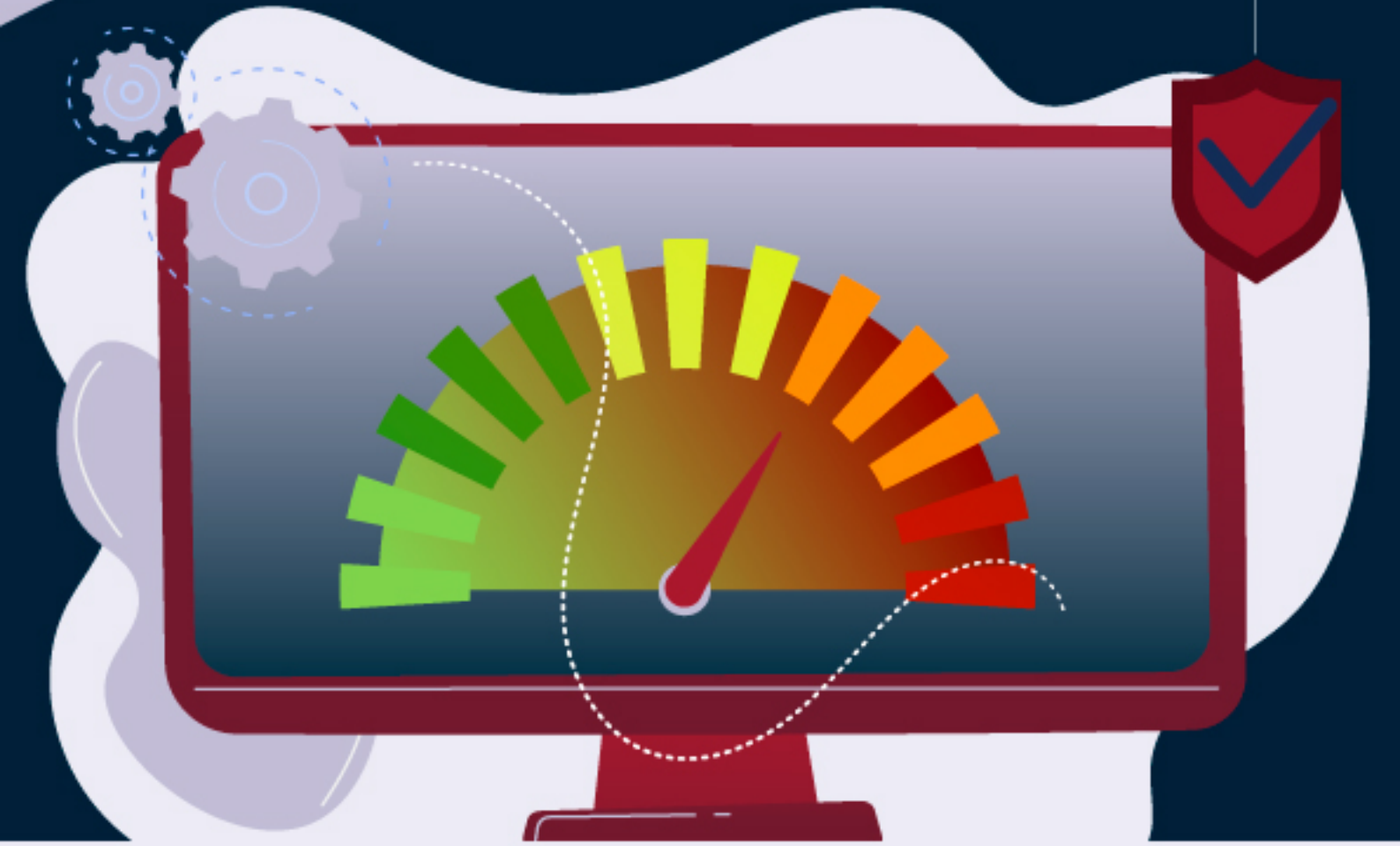
Indicador de madurez en ciberseguridad

OBSERVATORIO DE LA CIBERSEGURIDAD



isms forum INTERNATIONAL INFORMATION SECURITY COMMUNITY

isms BARCELONA INTERNATIONAL INFORMATION SECURITY COMMUNITY

Estudio sobre el nivel de madurez en ciberseguridad

Con la participación de los siguientes profesionales y organizaciones:

Coordinadores:

David Esteban

David Llorente

Iván Sánchez

María Guillamón

Olga Forné

Óscar Sánchez

Santiago Minguito

Toni García

Editor:

Daniel García Sánchez, Director General de ISMS Forum

Diseño y maquetación:

Raquel García Robles, Responsable de Comunicación Externa de ISMS Forum

ÍNDICE

01. ISMS Forum y su nueva iniciativa: el Observatorio de la Ciberseguridad 6

02. Estudio sobre el nivel de madurez en ciberseguridad de la empresa española 8

03. Aplicación de los dominios establecidos por el NIST 9

04. Principales indicadores 11

05.Anexo de Conclusiones 20

ISMS Forum y su nueva iniciativa: el Observatorio de la Ciberseguridad

ISMS Forum es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el sector. Creada con una vocación plural y abierta, se configura como el principal foro nacional especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. Toda su actividad se desarrolla en base a los valores de transparencia, independencia, objetividad y neutralidad.

ISMS Forum inició su andadura como Capítulo Español de ISMS International User Group (IUG), organización que promovía el conocimiento e implementación de los Sistemas de Gestión de la Seguridad de la Información en todo el mundo, de acuerdo con la familia de estándares ISO 27000. En la actualidad la Asociación mantiene representación global unificada y centralizada en España bajo la marca denominada International Information Security Community.

La Asociación organiza su actividad a través de distintas iniciativas, que abordan desde una perspectiva global o especializada la Seguridad de la Información: Jornadas Internacionales, Data Privacy Institute, Cloud Security Alliance, Cyber Security Center, IoT Security Center, workshops sobre materias concretas y formación especializada en protección de datos y ciberseguridad. Además gestiona las certificaciones Certified Data Privacy Professional (CDPP), Certificación de Delegado de Protección de Datos (CDPD), Certified Cyber Security Professional (CCSP) y promueve el Certificate Of Cloud Security Knowledge (CCSK).

En 2020, el marco asociativo de ISMS Forum se ha consolidado como la mayor comunidad de expertos y organizaciones con interés y responsabilidades en materia de seguridad de la información, promoviendo la formación y excelencia de sus asociados, facilitándoles cauces de interlocución con las administraciones y autoridades de control, y fomentando el intercambio de conocimientos entre los principales actores y expertos implicados en el sector para impulsar y contribuir a la mejora de la ciberseguridad en España.

Unido a lo anterior, la Asociación da un paso más con el objetivo crear un estado de conciencia sobre la necesidad de formar y sensibilizar, aportando indicadores que permitan gestionar los riesgos derivados de la dependencia actual de la sociedad respecto a las Tecnologías de la Información y la Comunicación (TIC), siendo un aspecto clave para asegurar el desarrollo socio-económico del país.

Para alcanzar la misión anteriormente descrita, la Asociación identifica la necesidad de actuar como referente y ofrecer una plataforma para el desarrollo de indicadores que permita la puesta en común y el análisis de aquellas áreas que generan mayor preocupación y, en general, de los riesgos y retos más relevantes. Se constituye de esta manera el primer Observatorio de la Ciberseguridad para empresas y profesionales del sector.

Objetivos del Observatorio de la Ciberseguridad

- Plataforma para el análisis del nivel de madurez, evolución y nuevos fenómenos en el ámbito de la seguridad de la información.
- Generación de indicadores nacionales sobre el estado de la Ciberseguridad en empresas y entidades privadas y públicas.
- Promoción de conocimiento e investigación.
- Generación de métricas y referencias nacionales.
- Colaboración e interlocución con instituciones y reguladores.

Estudio sobre el nivel de madurez en ciberseguridad de la empresa española

Según define la gestión de riesgos el Instituto Nacional de Estándares y Tecnología (NIST) de EEUU, se trata del proceso continuo de identificación, evaluación y respuesta al riesgo; y para gestionar el riesgo, las organizaciones deben comprender la probabilidad de que ocurra un evento y los posibles impactos resultantes. Esta es la premisa con la que ISMS Forum pone a disposición del mercado una herramienta de evaluación a través del primer indicador nacional de madurez en ciberseguridad con el que las organizaciones puedan determinar el nivel de riesgo que mantienen en comparación con la media establecida.

El Estudio sobre el nivel de madurez en ciberseguridad de la empresa española es el primer análisis que establece el Observatorio de la Ciberseguridad de ISMS Forum con la finalidad de generar claridad sobre el estado del arte de la ciberseguridad empresarial nacional y para facilitar información de utilidad para empresas y profesionales con la generación de un indicador anual que permita interpretar de una mejor manera la evolución interanual de los riesgos cibernéticos y su relación con terceros factores y fenómenos.

El indicador de nivel de madurez en ciberseguridad utiliza el marco metodológico basado en el estándar creado por el Instituto Nacional de Estándares y Tecnología (NIST) en 2013. Dicho marco ha sido globalmente utilizado por organizaciones de cualquier sector o tamaño, sirviendo de referencia a las organizaciones que apliquen los principios y buenas prácticas para medir y mejorar sus capacidades de Identificación, Protección, Detección, Respuesta y Recuperación. Cabe aclarar que NIST proporciona un marco de políticas de orientación de ciberseguridad no vinculantes, que cada organización deberá adaptar a sus necesidades, regulación aplicable y naturaleza propias.

El estudio realizado por ISMS Forum ha tenido por objeto la aplicación del Marco elaborado por NIST en una muestra formada por 100 directores de seguridad de la información que operan en el ámbito territorial nacional, tanto en empresas multinacionales como nacionales. No se ha recopilado información de empresas proveedoras de servicios de ciberseguridad.

Aplicación de los dominios establecidos por el NIST

Identificar

Gestión de activos, Entorno de negocios, Gobernanza, Evaluación de riesgos y Estrategia de gestión de riesgos.

Desarrollar una comprensión organizacional para administrar el riesgo de ciberseguridad para sistemas, personas, activos, datos y capacidades.

Proteger

Gestión de identidad y control de acceso, Conciencia y entrenamiento, Seguridad de datos, Procesos y procedimientos de protección de la información, Mantenimiento y Tecnología de protección.

Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos. La función Proteger admite la capacidad de limitar o contener el impacto de un posible evento de ciberseguridad.

Detectar

Anomalías y eventos, Monitoreo continuo de seguridad y Procesos de detección.

Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La Función Detectar permite el descubrimiento oportuno de eventos de ciberseguridad.

Responder

Planificación de respuesta, Comunicaciones, Análisis, Mitigación y Mejoras.

Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de ciberseguridad.

Recuperar

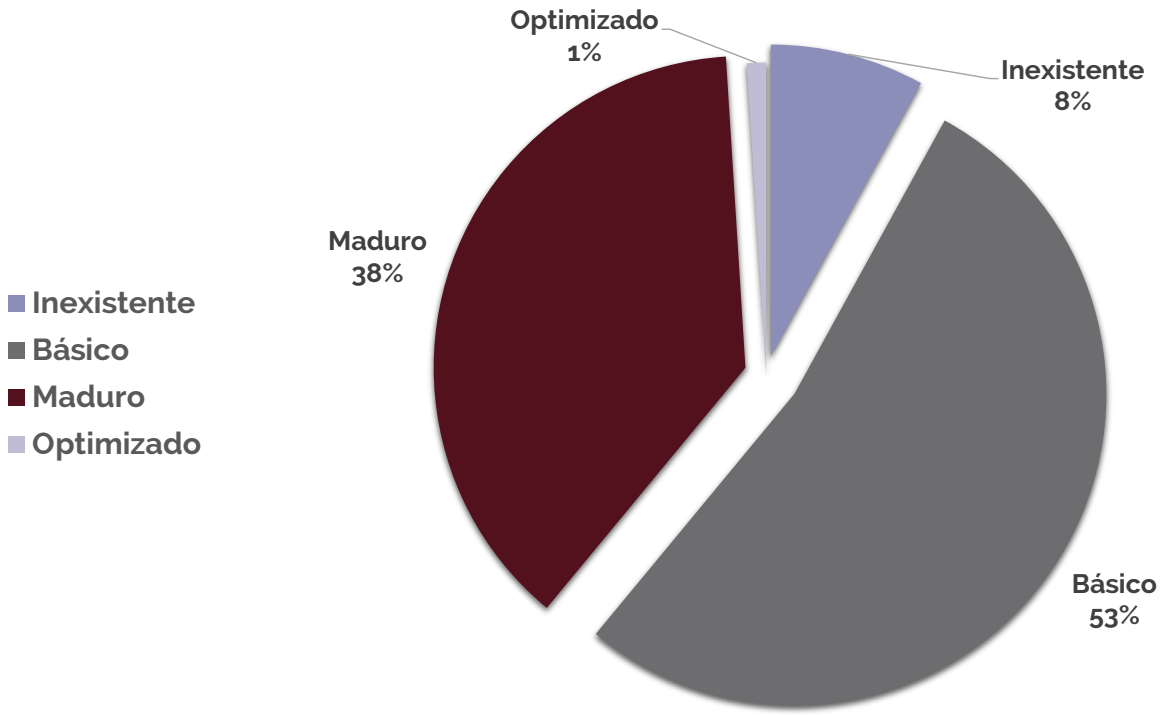
Planificación de recuperación, Mejoras y Comunicaciones.

Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de ciberseguridad.

Principales indicadores

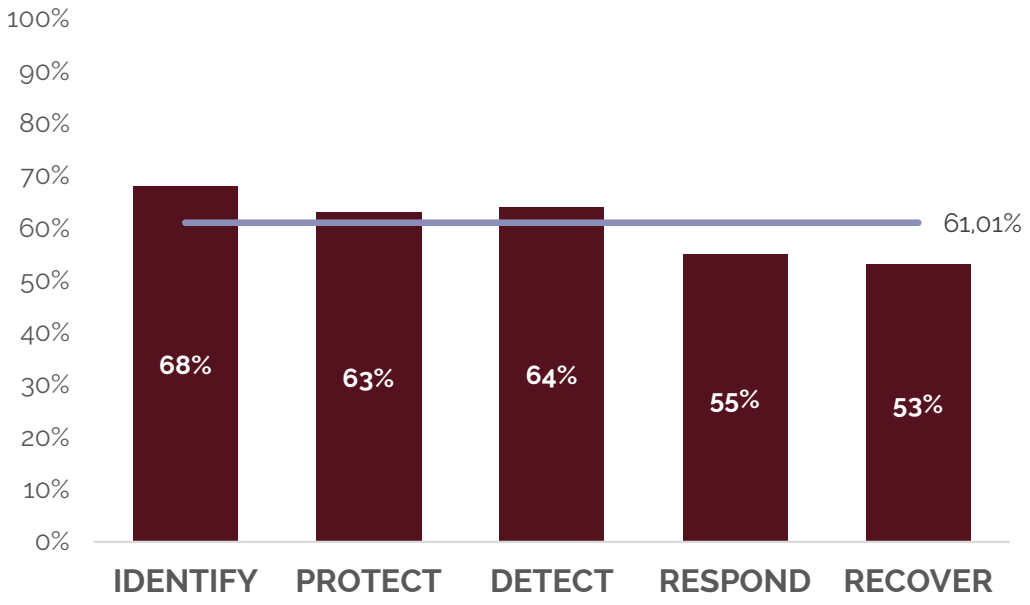
Se inicia la exposición de resultados del presente Estudio con el análisis del grado de madurez global reflejado en el indicador.

Grado de madurez



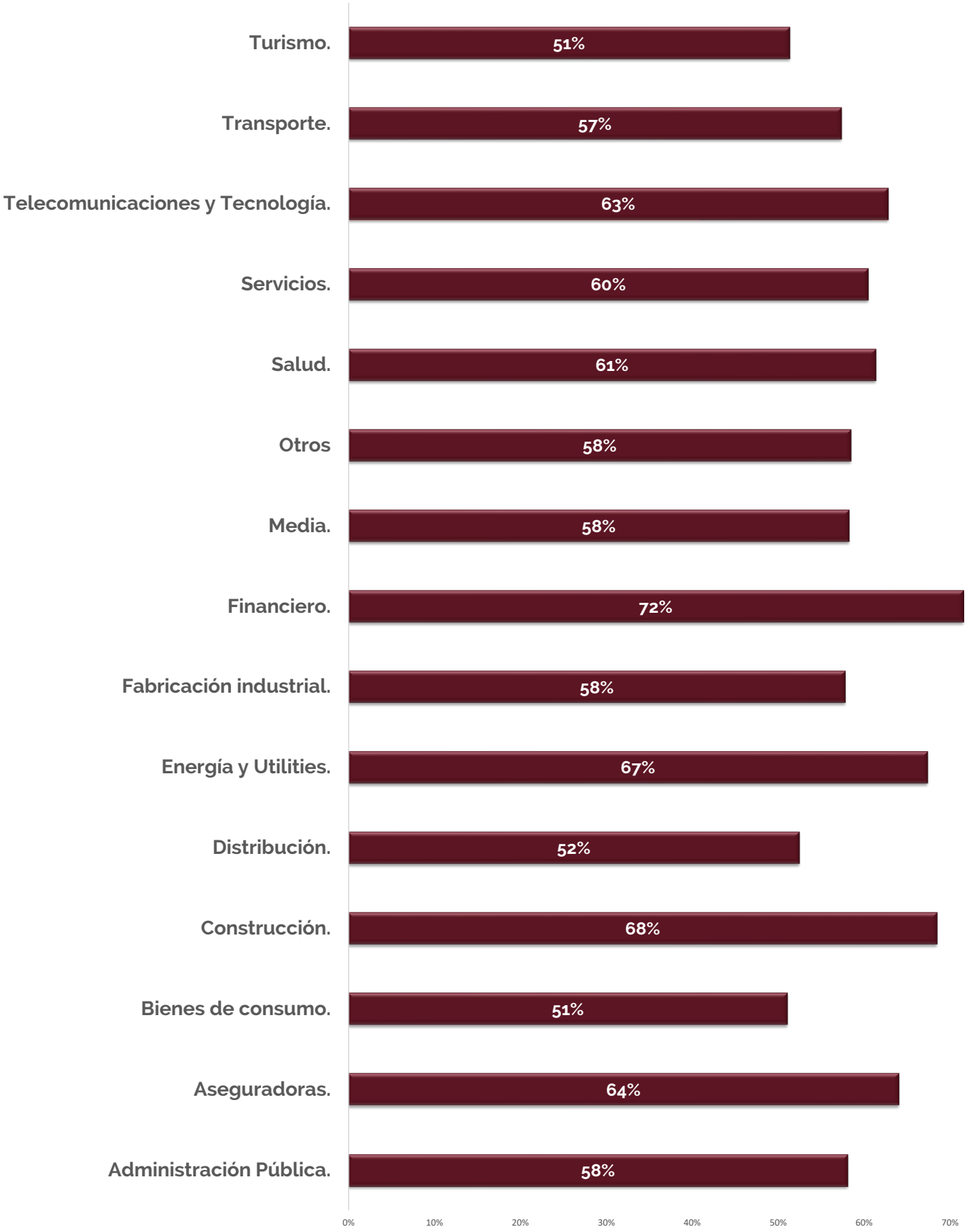
Nivel de Madurez por Dominio NIST

Sector	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER	Nivel de madurez
Financiero.	76%	74%	79%	63%	66%	72%
Construcción.	76%	70%	61%	67%	67%	68%
Energía y Utilities.	77%	65%	72%	68%	50%	67%
Aseguradoras.	73%	63%	67%	58%	58%	64%
Telecomunicaciones y Tecnología.	79%	68%	58%	53%	50%	63%
Salud.	69%	67%	62%	50%	58%	61%
Servicios.	69%	68%	57%	48%	58%	60%
Otros	61%	63%	60%	55%	50%	58%
Media.	64%	63%	61%	56%	37%	58%
Administración Pública.	64%	62%	67%	48%	48%	58%
Fabricación industrial.	67%	58%	64%	52%	44%	58%
Transporte.	62%	55%	65%	58%	44%	57%
Distribución.	58%	35%	61%	57%	63%	52%
Turismo.	50%	57%	63%	39%	50%	51%
Bienes de consumo.	52%	52%	51%	51%	46%	51%

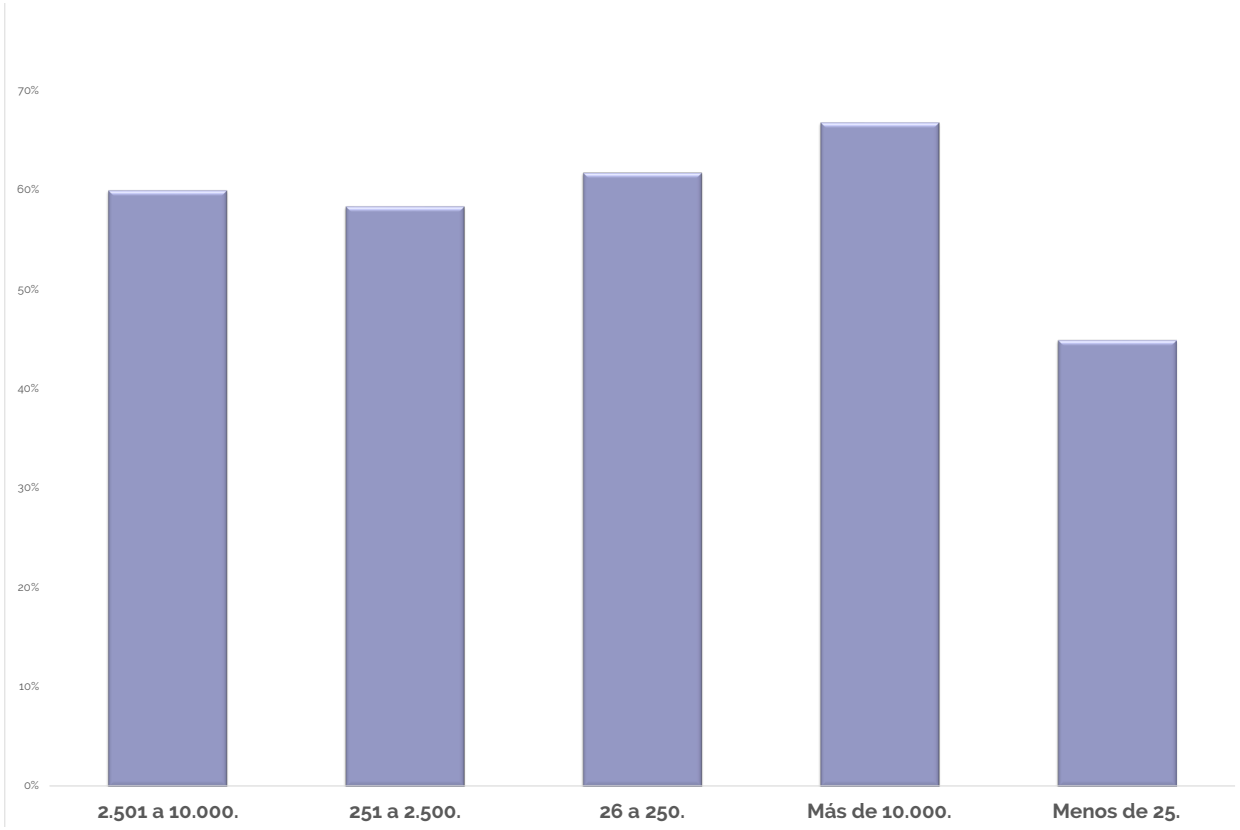


- El promedio de todos los dominios se sitúa en la franja alta de madurez básica.
- Destacan los ámbitos de Identify y Detect, seguido de Protect.
- Respond y Recovery son los dominios que muestran una clara necesidad de mejora.

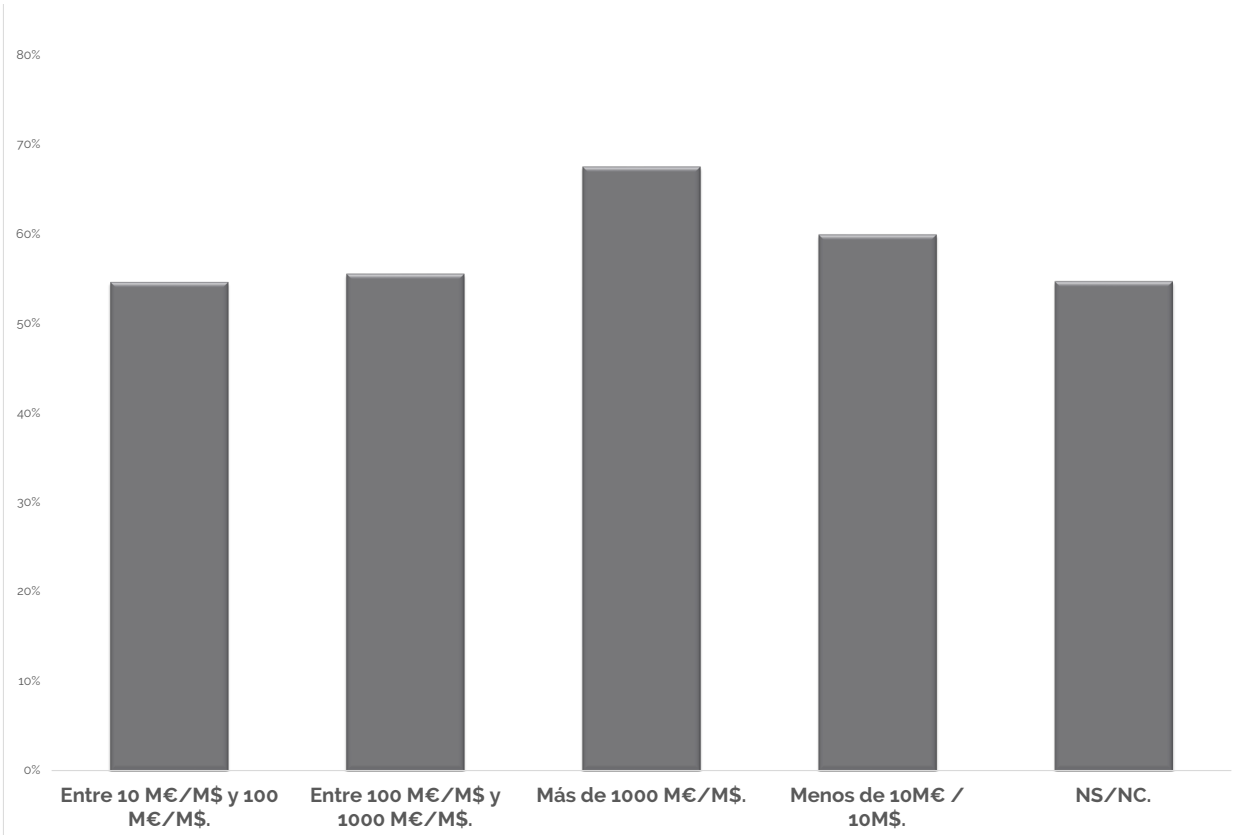
Grado de madurez por sector



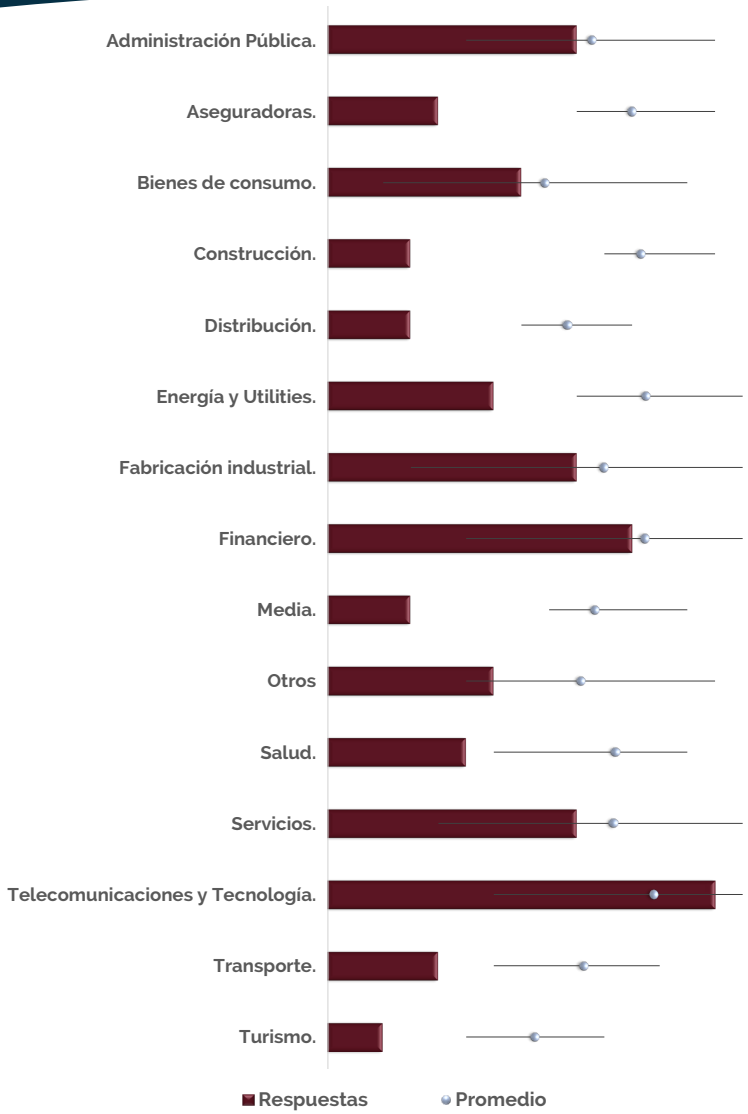
Grado de madurez por número de empleados



Grado de madurez por facturación

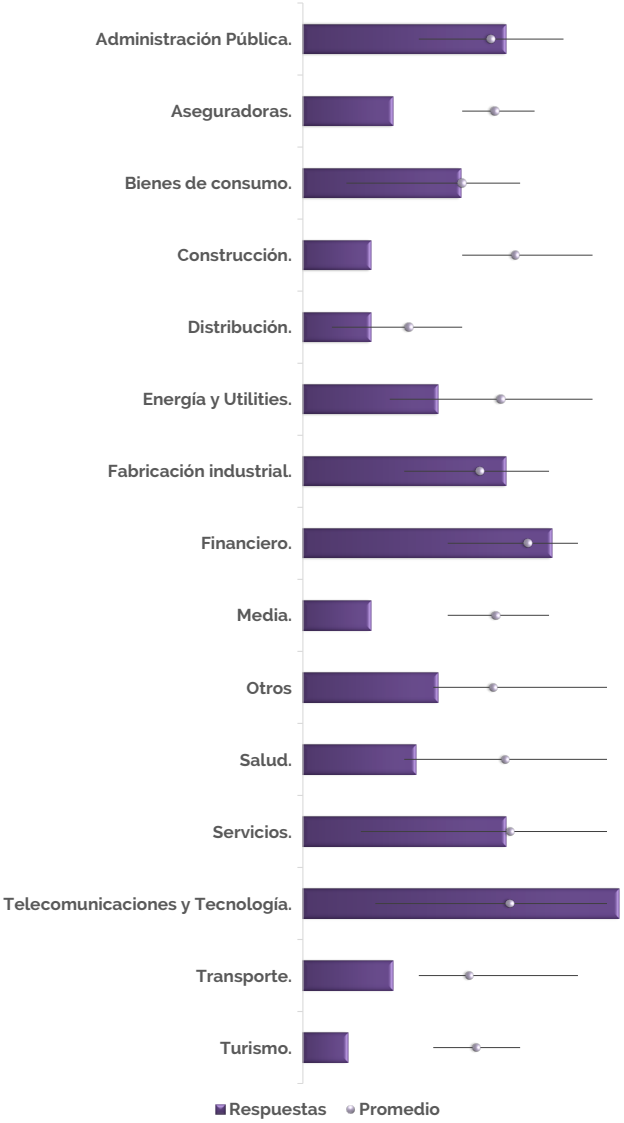


DOMINIO 1: Identificar



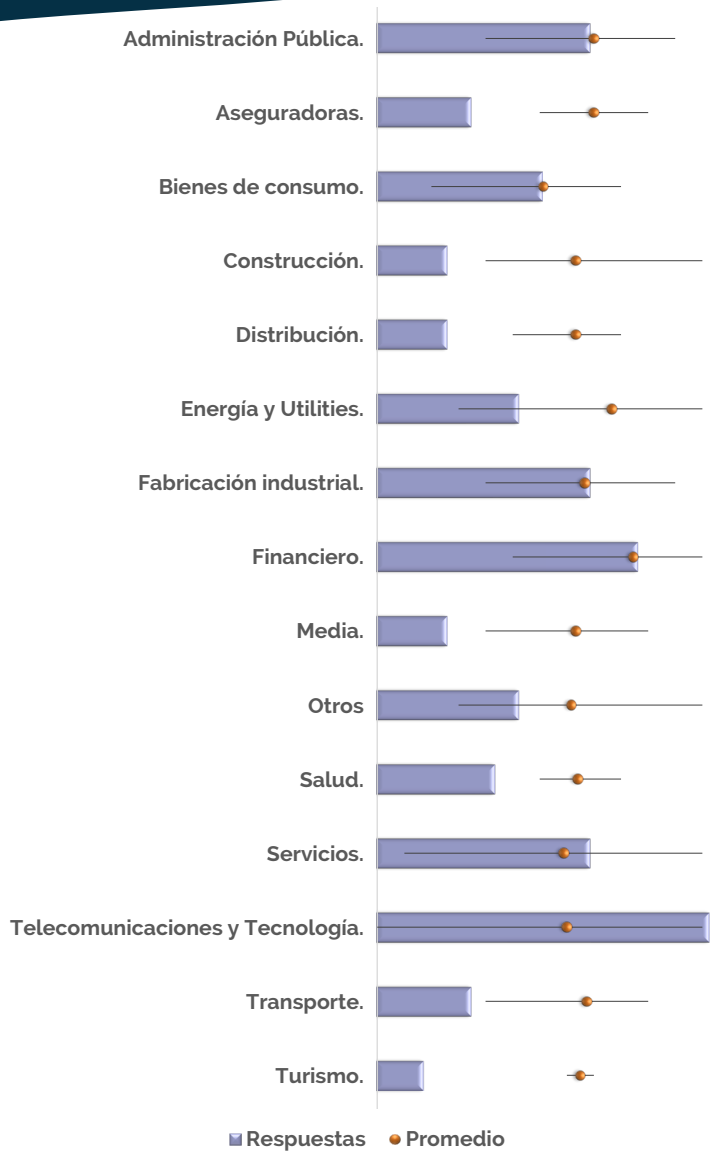
- Sector Telecomunicaciones y Tecnología, y Financiero, muestran mayor madurez, teniendo en cuenta la representación de la muestra.
- Les siguen Energía y Utilities, Construcción y Aseguradoras, si bien la representación es menor.
- Destacar la dispersión de la respuesta en los sectores de Fabricación Industrial y Bienes de Consumo.

DOMINIO 2: Proteger



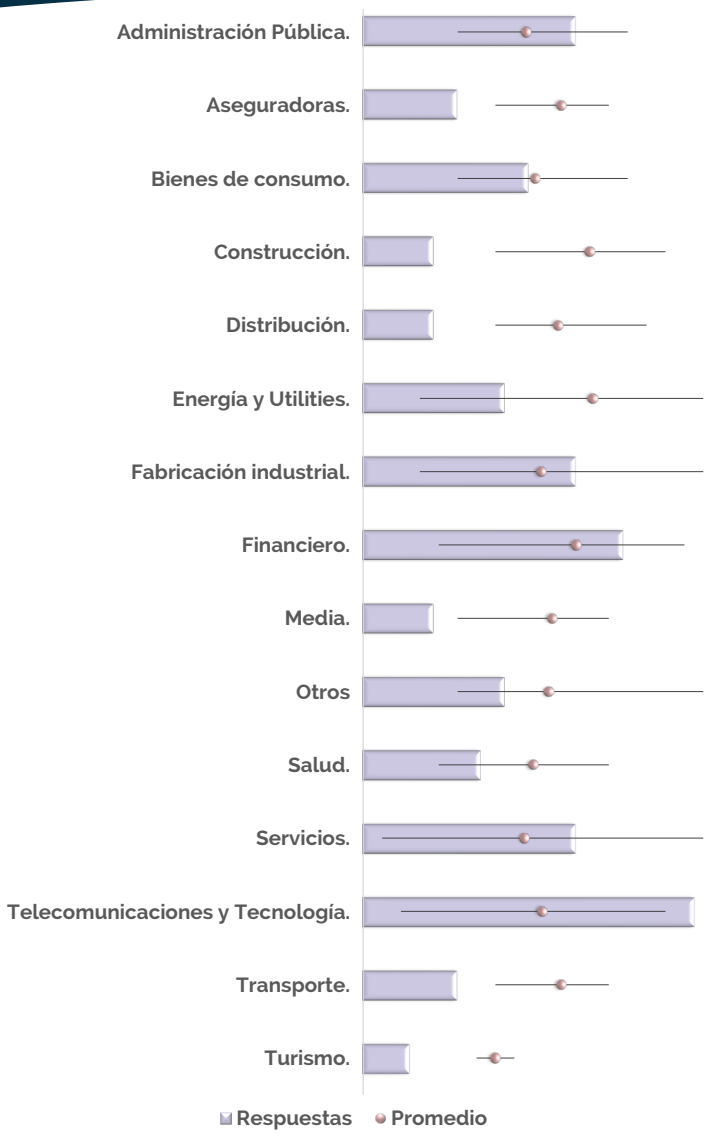
- Sector Financiero lidera el dominio de Protect.
- En general el nivel de madurez es similar en todos los sectores analizados, excepto en Distribución (si bien su representación en la muestra es baja).
- Destacar la dispersión de la respuesta el sector de Servicios.

DOMINIO 3: Detectar



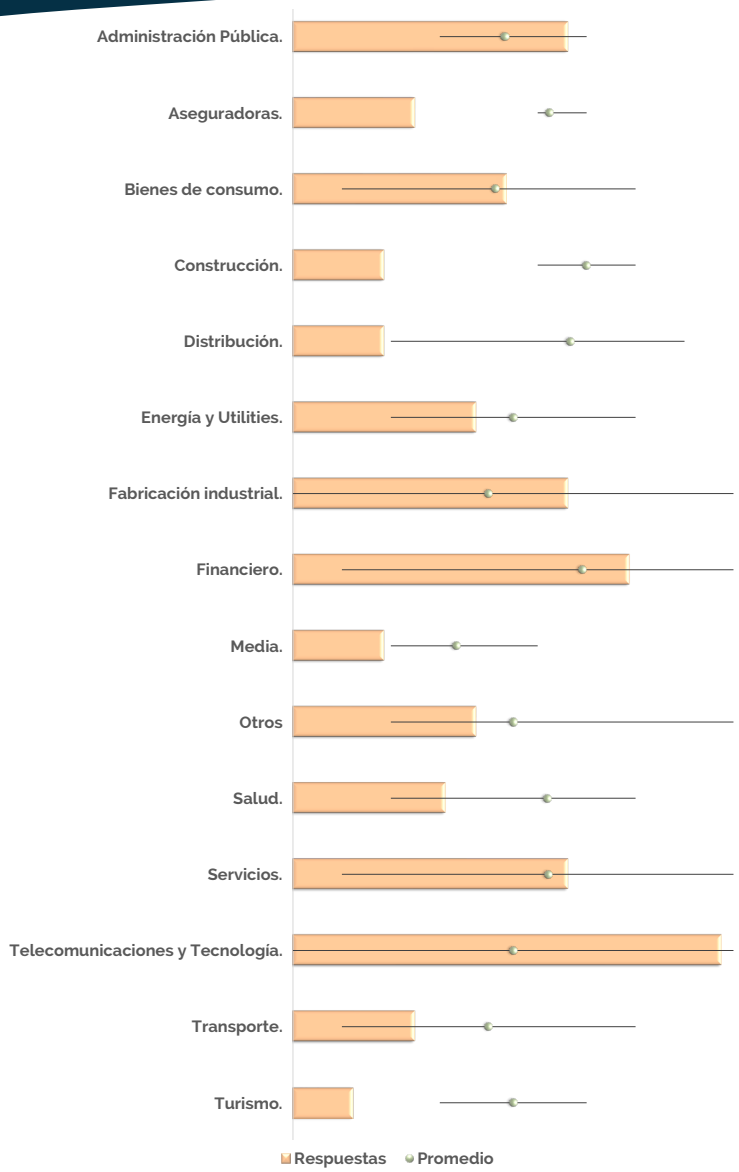
- El Sector Financiero lidera el dominio de Detect junto con Energía y Utilities.
- En el resto de sectores analizados el nivel de madurez es similar.
- Destacar la dispersión de la respuesta en el sector de Telecomunicaciones y Tecnología.

DOMINIO 4: Responder



- Energía y Utilities, y Construcción lideran el dominio de Respond, si bien su representación en la muestra es baja.
- En el resto de sectores analizados el nivel de madurez es similar, excepto en Turismo.
- Destacar la dispersión de la respuesta en el sector de Servicios.

DOMINIO 5: Recuperar



- Bienes de Consumo, Fabricación Industrial y Media son los sectores que muestran menor madurez en el ámbito de Recover.
- Destacar la dispersión de la respuesta en los sectores de Fabricación Industrial, y Telecomunicaciones y Tecnología.

Anexo de Conclusiones

IDENTIFICAR

El inventario de dispositivos, sistemas, aplicaciones y recursos de información, y gestión de roles y responsabilidades, solo es completo en un tercio de la muestra.
Cerca del 50% de las empresas identifican y comunican las dependencias y los requisitos de los servicios y funciones críticas, asociadas a la misión, visión y objetivos de la organización.

Más del 60% de las empresas cuentan con una política donde se definen los roles y responsabilidades, junto con los requerimientos legales y regulatorios, dentro del marco de los procesos de gobierno y gestión del riesgo de ciberseguridad.

Hasta un 50% de las empresas mantienen identificadas y documentadas las vulnerabilidades y amenazas de ciberseguridad, y analizan el riesgo en base a la probabilidad e impacto en el negocio.

Solo el 30% de la muestra manifiesta que los procesos de gestión del riesgo, así como el nivel de tolerancia, están establecidos, gestionados, acordados e informados con las partes interesadas.

En relación a los procesos de gestión del riesgo de la cadena de subministro (proveedores y terceros), predomina (40%) la existencia de un proceso de gestión del riesgo de terceros y el establecimiento de las medidas en los contratos, pero no se auditan.

PROTEGER

Casi la mitad de las empresas encuestadas manifiesta la existencia de una gestión de identidades y accesos en base al principio de menor privilegio y segregación de funciones.

En materia de formación y concienciación, el grupo mayoritario presenta una formación que llega a todos los empleados pero que se realiza anualmente.
En la gestión del ciclo de vida del dato, más del 50% de las entidades identifican los datos pero los protegen de manera parcial.

En cuanto a la protección de los sistemas y activos de información, más del 40% de las empresas participantes manifiesta documentar los procesos y procedimientos, pero no la implementación de todos ellos.

La mitad de los encuestados afirma la realización de un mantenimiento de los sistemas de información y control industrial, pero manifiesta que no se auditan los accesos.

Más del 50% de las entidades dispone de medidas técnicas de seguridad, y solo un 20% declara medidas técnicas completas, asociadas a la política y procedimientos de seguridad, que proporcionen seguridad y resiliencia a los sistemas y activos de información.

DETECTAR

En la recolección de eventos, predominan el uso de sistemas para la recolección de eventos para los sistemas y redes clave del negocio.

Más del 40% de las empresas realiza un análisis de comportamiento para la detección de actividades anómalas mediante métodos automáticos en función de umbrales definidos.
En la identificación de eventos de seguridad, la opción mayoritaria supone la monitorización de la actividad de los usuarios o dispositivos en los sistemas críticos de negocio bajo demanda.

En el 50% de las empresas, los procedimientos de detección están definidos, aunque no todas las responsabilidades se encuentran asignadas. Se llevan a cabo pruebas 1 vez al año.

RESPONDER

En el 50% de las entidades, los procedimientos de respuesta ante incidentes de ciberseguridad están documentados, actualizados y se prueban con carácter anual.

La opción mayoritaria muestra que los principales procesos, roles e interlocutores en la comunicación de respuesta ante incidentes están identificados. Se les forma y capacita de manera regular (1 vez al año). La comunicación y coordinación es ad-hoc.

El grueso de empresas participantes investiga las alertas más relevantes generadas por los sistemas de detección de acuerdo a un proceso definido, pero sin SLAs formalizados.

Tras un incidente de seguridad, cabe destacar la gran disparidad a la hora de realizar un análisis forense de eventos detectados (en la opción más común, inferior al 10% de las detecciones).

En cuanto a la identificación temprana de vulnerabilidades y amenazas, la mitad de la muestra la realiza mediante procesos automáticos. Los procesos de contención y mitigación son manuales.

Gran disparidad en las acciones de mejora continua de la respuesta ante incidentes. Solo un 8% revisa los planes de respuesta más de una vez al año y hasta un 36% lo hace únicamente ad hoc.

RECUPERAR

Los planes de recuperación de los sistemas clave de negocio ante incidentes de ciberseguridad se encuentran formalizados, pero no se siguen paso a paso por la organización y en muchos casos se revisan ad hoc.

En la mitad de las empresas encuestadas, los planes y estrategias de recuperación se actualizan anualmente y se incorporan lecciones aprendidas.

Las actividades y roles en la comunicación (interna y externa) durante un proceso de recuperación están definidos, pero la mitad de las empresas manifiesta la existencia de canales informales para la comunicación.

Más información en:
www.ismsforum.es

 @ISMSForum

 ISMS Forum

isms forum | INTERNATIONAL INFORMATION SECURITY COMMUNITY