CENTRO DE CIBERSEGURIDAD INDUSTRIAL

Check Point
SOFTWARE TECHNOLOGIES LTD.

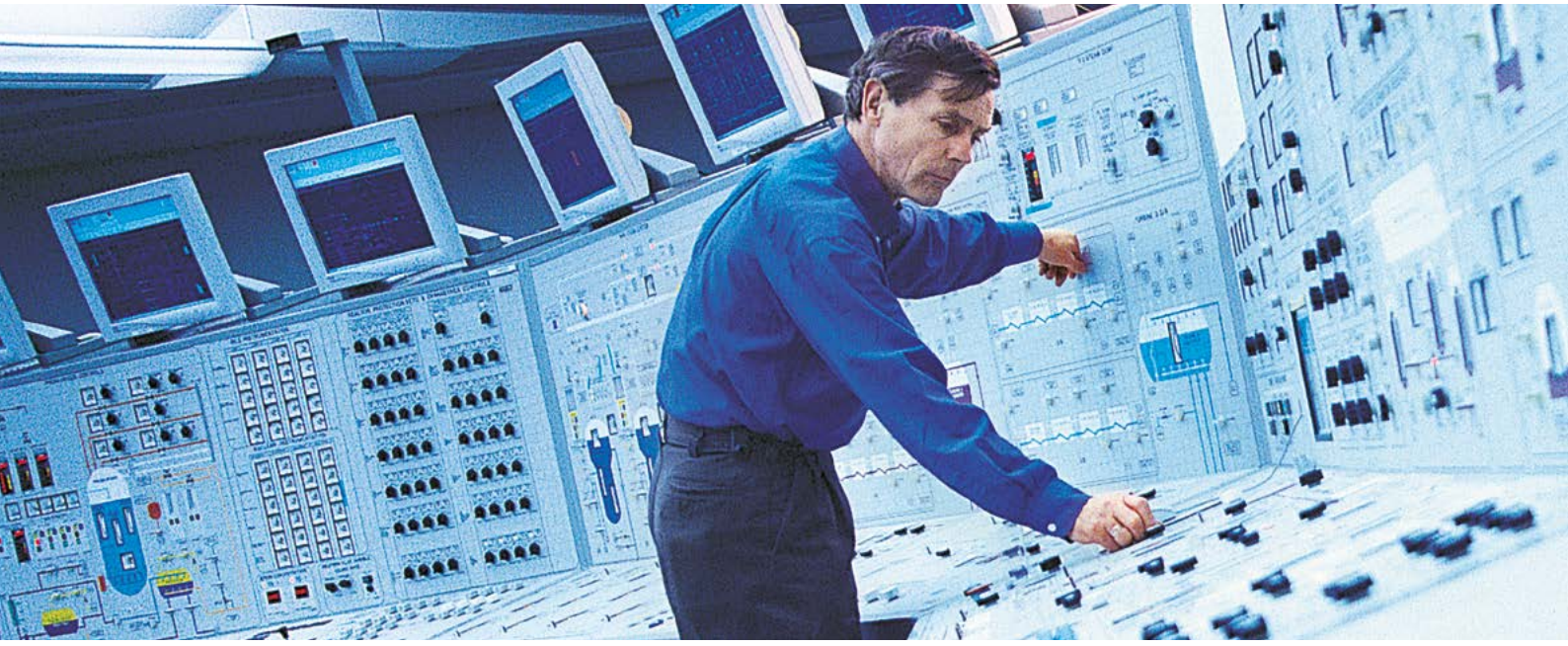
INCIDENTES DE CIBERSEGURIDAD INDUSTRIAL EN SERVICIOS ESENCIALES DE ESPAÑA.

EDICIÓN 2019

PROMOVIENDO UN ESCENARIO DE CONFIANZA EN ESPAÑA

El Centro de Ciberseguridad Industrial (CCI) es una organización independiente, sin ánimo de lucro, cuya misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial desarrollando actividades de análisis, desarrollo de estudios e intercambio de información sobre el conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, y cómo éstas suponen una de las bases sobre las que está construida la sociedad actual.

CCI es el punto de encuentro, independiente, para los organismos, privados y públicos, y los profesionales relacionados con las prácticas y tecnologías de la Ciberseguridad Industrial; así como la referencia hispanohablante para el intercambio de conocimiento y experiencias y para la dinamización de los sectores involucrados en este ámbito.



Edición: mayo 2019

ISBN: 978-84-947727-9-5

Paseo de las Delicias, 30 · 2º piso
28045 MADRID
+34 910 910 751
info@CCI-es.org
www.CCI-es.org
blog.CCI-es.org
@info_CCI

Check Point Software Technologies Ltd. (www.checkpoint.com), es el mayor proveedor mundial especializado únicamente en seguridad, que proporciona soluciones líderes en la industria y protege a los clientes de ciberataques con una tasa inigualable de capturas de malware y otros tipos de amenazas. Check Point ofrece una completa arquitectura de seguridad para defender desde las redes empresariales hasta los dispositivos móviles, además de la gestión de la seguridad más intuitiva e integral. Check Point protege más de 100.000 organizaciones de todos los tamaños.

En colaboración con

Check Point
SOFTWARE TECHNOLOGIES LTD.

www.checkpoint.com
CheckPoint Software España
@CheckPointSpain

Consejos

Alt+flecha izquierda para volver a la vista anterior después de ir a un hipervínculo

Haz click en nuestro icono y visita nuestra web

Haciendo click en la banderas de la portada podrás ver la actividad de CCI en cada uno de esos países

Haciendo click en el título de la cabecera volverás al índice

Patrocinadores del CCI

Platinum

Eleven Paths

Telefónica

Gold

Accenture Security

Check Point Software Technologies Ltd.

Cisco

Entelgy Innotec Security

Fortinet

paloalto Networks

Silver

Capsa Food

dimension data

Kaspersky Lab

S21sec

Siemens

Sothis

Tecnicas Reunidas

Trend Micro

TSK Grupo

TÜVIT TÜV NORD GROUP

Bronze

axians

Atos

CIC Consulting Informático

Eulen Seguridad

everis

Forescout

gmv Innovating Solutions

Logitek

Getronics

Nozomi Networks

nunsys Tu socio tecnológico

oylo Trust Engineering

Phoenix Contact

S2 Grupo

sia

tecnalia Inspiring Business

INTRODUCCIÓN

Durante 2018, se han registrado mas de 33.000 incidentes de ciberseguridad en entidades del sector público y empresas de interés estratégico para España, una cuarta parte más que el año anterior, según el Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia (CNI). De dichos ataques, alrededor de 1.600 han sido calificados de peligrosidad muy alta.

La Directiva NIS (Directiva de la UE 2016/1148) del Parlamento Europeo y sus correspondientes transposiciones al ordenamiento jurídico español, así como la RGPD y el real decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información promulgan la gestión de incidentes de ciberseguridad como una imposición legal para todas las organizaciones públicas y algunas privadas de España que prestan servicios esenciales. El Consejo Nacional de Ciberseguridad de España ha aprobado recientemente la Guía Nacional de Notificación y Gestión de Ciberincidentes, la primera de toda la Unión Europea. Esta guía incluye una descripción detallada del proceso de notificación, con 38 tipos de ataques, agrupados en 10 clases y 5 correspondientes a niveles de peligrosidad, así como 6 de impacto.

La Guía Nacional de Notificación y Gestión de Ciberincidentes permitirá a las entidades públicas y privadas conocer a quién se tienen que dirigir y los pasos a seguir, así como a implementar conceptos de Gestión de Incidentes, de forma equivalente a como se establece en la norma ISO 27035.

Esta guía elaborada de forma conjunta por los Equipos de Respuesta a Incidentes de Seguridad del Gobierno de España: **CCN-CERT,** del Centro Criptológico Nacional del Centro Nacional de Inteligencia; **Incibe-CERT,** del Instituto Nacional de Ciberseguridad de España; **CNPIC** (Centro Nacional de Protección de Infraestructuras y Ciberseguridad); y **Espdef-CERT** del Mando Conjunto de Ciberdefensa contiene la información necesaria para la contención y resolución de incidentes de Seguridad a través de las correspondientes herramientas de notificación y ticketing.

Este estudio analiza los incidentes de ciberseguridad en operadores de servicios esenciales en base a los resultados de 18 entrevistas realizadas en 2019 a representantes de operadores de cinco sectores estratégicos. Las preguntas de las entrevistas han sido diseñadas para obtener una visión precisa de cuál es el estado de situación en la gestión de incidentes en las empresas que operan servicios esenciales.

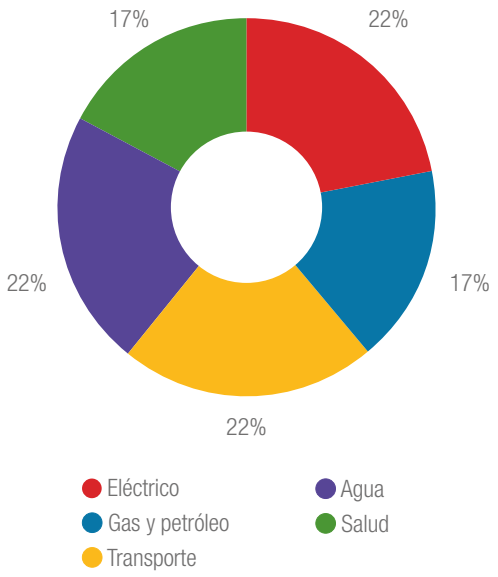


Gráfico 1 – Porcentaje de Sectores Participantes.

ESTUDIO SOBRE EL ESTADO DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD INDUSTRIAL EN OPERADORES DE SERVICIOS ESENCIALES

DESCRIPCIÓN DE LA ENCUESTA

Este estudio se ha realizado a partir de las entrevistas a responsables de organizaciones que operan servicios esenciales, analizándose las respuestas facilitadas.

Este documento muestra los resultados de dichas entrevistas y proporciona interpretaciones a las mismas basadas en el conocimiento y experiencia de sus redactores. Queda a criterio del lector sacar sus propias conclusiones.

TIPOLOGÍA DE INCIDENTES

¿Qué tipo de incidentes tecnológicos conoce en la operación de servicios esenciales con alto impacto?

Los incidentes pueden ser intencionados o no. La mayoría son provocados por fallos del software o un error humano por falta de concienciación o formación. En los incidentes intencionados es muy importante entender bien los pasos ejecutados por un malware o por los atacantes, ser conscientes de los equipos comprometidos y los procesos afectados, saber quién es el responsable del ataque, cuales ha sido las vías de entrada (paciente cero) y de propagación, sí la amenaza está acotada o sigue extendiéndose, y los riesgos identificados (operativo, financiero, medioambiental, seguridad de los trabajadores, reputación pública) son objetivos a los que debe dar respuesta el Centro de operaciones de seguridad (SOC) gracias a las tareas ejecutadas por los diferentes equipos que lo conforman.

En cuanto a la tipología de incidentes conocidos en servicios esenciales, los datos obtenidos señalan que más del 50% de los entrevistados conocen incidentes ocasionados por malware o ataques dirigidos, en cambio solo el 7% conoce incidentes que han comprometido información y un 4% conoce incidentes por fraude en servicios esenciales.

TIPOLOGÍA DE INCIDENTES CONOCIDOS EN SERVICIOS ESENCIALES

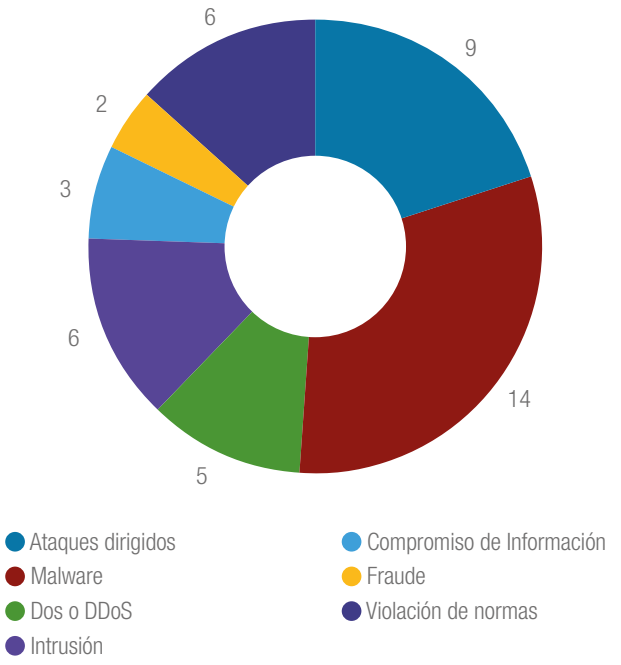


Gráfico 2 – Operadores de servicios esenciales: Tipo de incidentes conocidos.

Sector Eléctrico

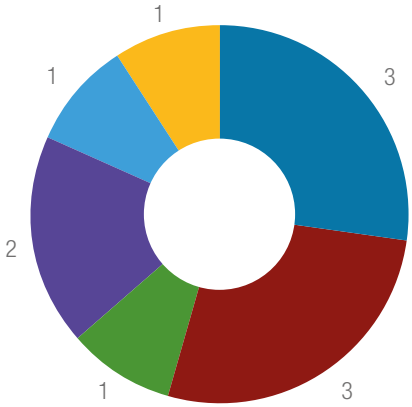


Gráfico 3 – Operadores del sector Eléctrico: Tipo de incidentes conocidos.

Sector Gas y Petróleo

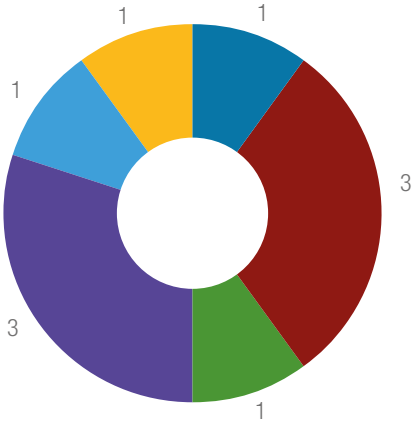


Gráfico 4 – Operadores del sector Gas y Petróleo: Tipo de incidentes conocidos.

Sector Agua

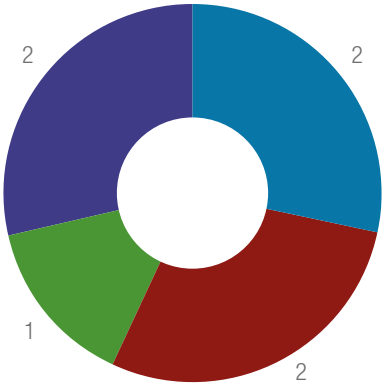


Gráfico 5 – Operadores del sector Agua: Tipo de incidentes conocidos.

Sector Salud

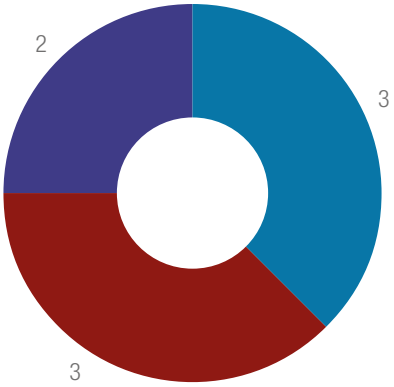


Gráfico 6 – Operadores del sector Salud: Tipo de incidentes conocidos.

Sector Transporte

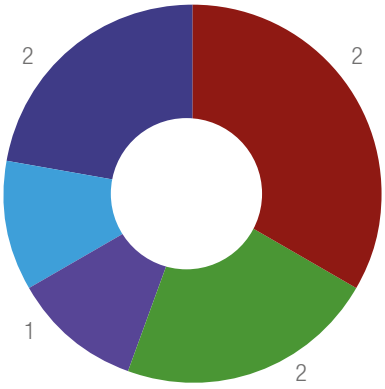


Gráfico 7 – Operadores del sector transporte: Tipo de incidentes conocidos.

Separada la información de las encuestas por sectores podemos observar que los responsables de sectores donde más tipos distintos de incidentes se conocen son del sector Eléctrico, Gas & Petróleo, y los responsables que menos incidentes conocen son del sector agua y salud.

- Ataques dirigidos
- Malware
- Dos o DDoS
- Intrusión
- Compromiso de Información
- Fraude
- Violación de normas

FUTUROS INCIDENTES DE CIBERSEGURIDAD

¿Qué incidentes en la operación de servicios esenciales espera que se produzcan en los próximos años?

Un 41% de las organizaciones que han participado en la encuesta están convencidos de que en un futuro próximo un número importante de los incidentes que se producirán serán debidos a que los dispositivos IoT serán comprometidos.

Esto ya está ocurriendo según algunos estudios que indican que España fue el objetivo de más del 70% de los ciberataques a dispositivos IoT en la primera mitad de 2018 o que ha sido el país que más ciberataques ha sufrido a través de dispositivos IoT durante varios meses.

Según un informe reciente de Check Point , a medida que el ecosistema de IoT se expande, también lo hace la superficie de ataque para los delincuentes cibernéticos. En otras palabras, cuanto más dependemos de la tecnología conectada en nuestras vidas diarias, más vulnerables somos a las amenazas que cada vez se adaptan más para explotar las vulnerabilidades y fallos en el diseño de seguridad en dispositivos IoT.

INCIDENTES FUTUROS

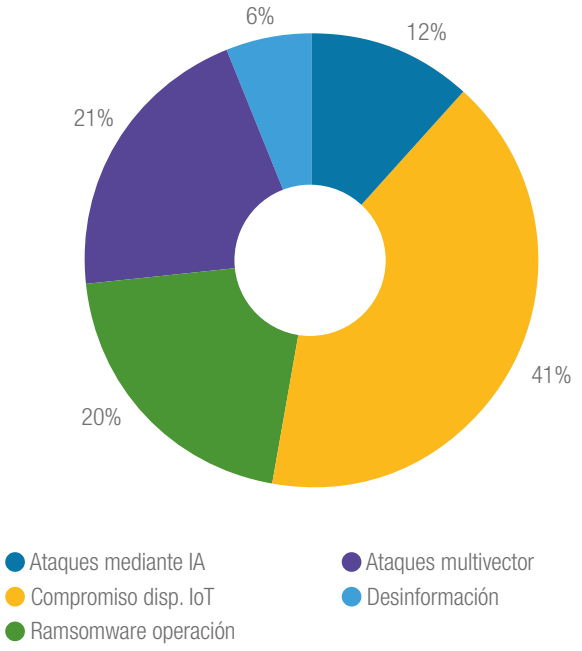


Gráfico 8 – Operadores de servicios esenciales: Incidentes futuros.

Sector Eléctrico

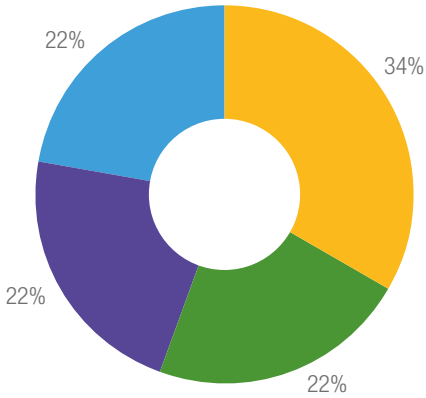


Gráfico 9 – Operadores del sector Eléctrico: Incidentes futuros.

Sector Gas y Petróleo

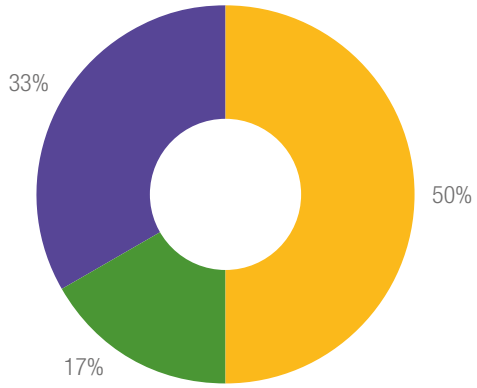


Gráfico 10 – Operadores del sector Gas y Petróleo: Incidentes futuros.

Sector Agua

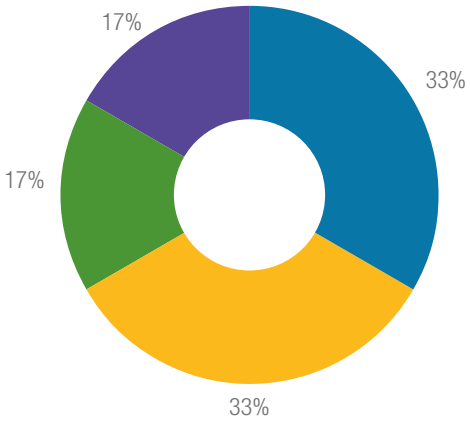


Gráfico 11 – Operadores del sector Agua: Incidentes futuros.

Sector Salud

Gráfico 12 – Operadores del sector Salud: Incidentes futuros.

Sector Transporte

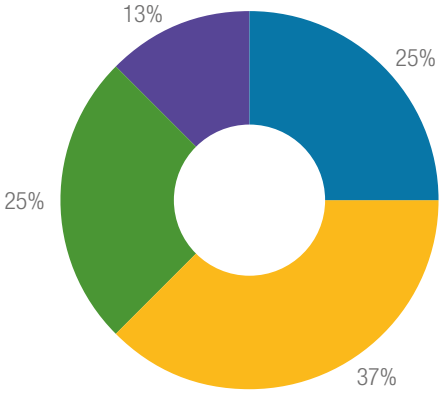


Gráfico 13 – Operadores del sector Transporte: Incidentes futuros.

De todos los sectores analizados, podemos destacar que los representantes de todos los sectores consideran que el compromiso de dispositivos IoT será la principal causa de incidentes en un futuro, también se puede destacar que todos consideran en menor porcentaje los ataques multivector y el ramsomware de operación será tipos de incidentes futuros.

- Ataques mediante IA
- Ataques multivector
- Compromiso disp. IoT
- Desinformación
- Ramsomware operación

CONOCIMIENTO DEL ORIGEN Y CONSECUENCIAS DE LOS INCIDENTES

¿Cuál es su grado de conocimiento sobre el origen, sistemas afectados y consecuencias de incidentes en operadores de servicios esenciales?

Cuando se produce un incidente en un entorno industrial, la disponibilidad de las operaciones, así como el buen funcionamiento de los sistemas que automatizan las protecciones *(safety),* son lo más importante. Por ello, la coordinación entre el centro de operaciones y la organización afectada debe quedar preestablecida en diferentes documentos para garantizar la continuidad del negocio en caso de un incidente. Disponer de un catálogo de los activos y procesos críticos, las personas de contacto necesarias para la gestión del incidente, el modelo de comunicación entre Comité de crisis, SOC y terceros, así como los tiempos de respuesta admisibles y contramedidas en caso de incidente.

Para lograr estar bien preparados en la respuesta es clave el conocimiento del origen, sistemas afectados y consecuencias de incidentes en este tipo de entornos que permitan realizar simulacros que pongan a pruebas las capacidades de respuesta.

Un 80% de los profesionales de operadores esenciales entrevistados señalan que conocen el origen, sistemas afectados y consecuencias de incidentes públicos sobre organizaciones que prestan servicios esenciales y más del 50% reconocen que conocen incidentes de su sector, e incluso propios. Este tipo de conocimiento es fundamental como ya hemos apuntado.

CONOCIMIENTO DE ORIGEN Y CONSECUENCIAS

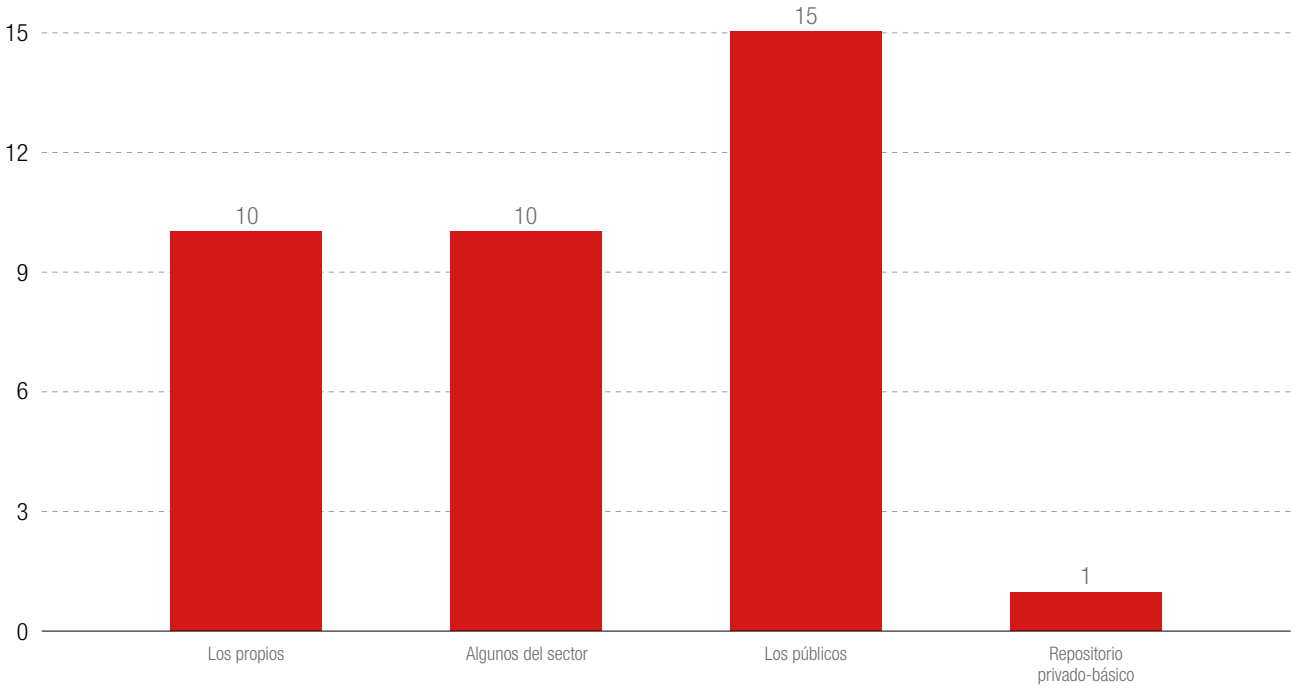


Gráfico 14 – Operadores de servicios esenciales: Conocimiento de origen y consecuencias.

Sector Eléctrico

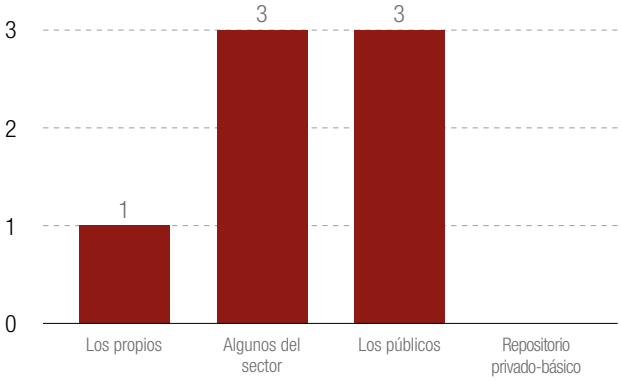


Gráfico 15 – Operadores del sector Eléctrico: Conocimiento de origen y consecuencias.

Sector Gas y Petróleo

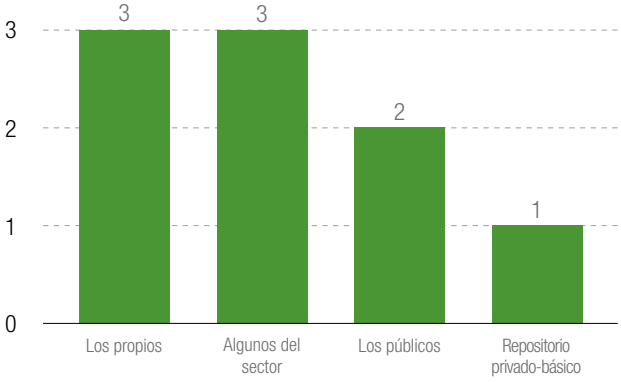


Gráfico 16 – Operadores del sector Gas y Petróleo: Conocimiento de origen y consecuencias.

Sector Agua

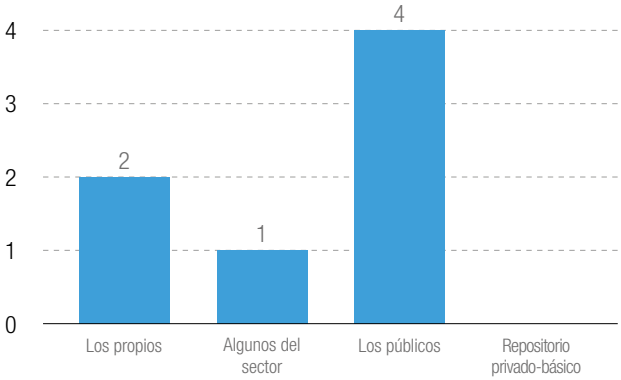


Gráfico 17 – Operadores del sector Agua: Conocimiento de origen y consecuencias.

Sector Salud

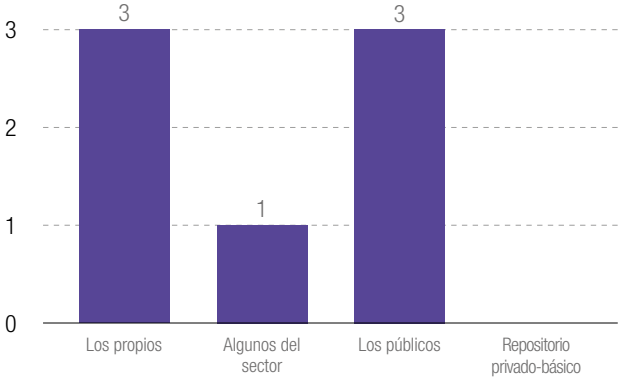


Gráfico 18 – Operadores del sector Salud: Conocimiento de origen y consecuencias.

Sector Transporte

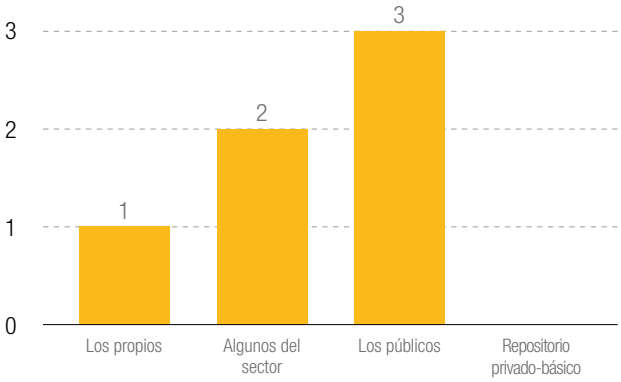


Gráfico 19 – Operadores del sector Transporte: Conocimiento de origen y consecuencias.

INCIDENTES CONOCIDOS DEL SECTOR

¿Cuál es el tipo de incidentes en operadores de su sector que conoce?

Las organizaciones están incorporando cada vez mejores medidas de Ciberseguridad; entre las medidas técnicas, más habituales están los antivirus, *firewalls* convencionales, IDS/IPS, auditorias de seguridad internas y gestión de respuesta a incidentes. La tipología de incidentes varía en función del sector como podemos apreciar dentro de los apartados de diferentes sectores, pero se puede concluir que los incidentes causados por malware son los más habituales.

TIPOLOGÍA DE INCIDENTES EN SU SECTOR ESENCIAL

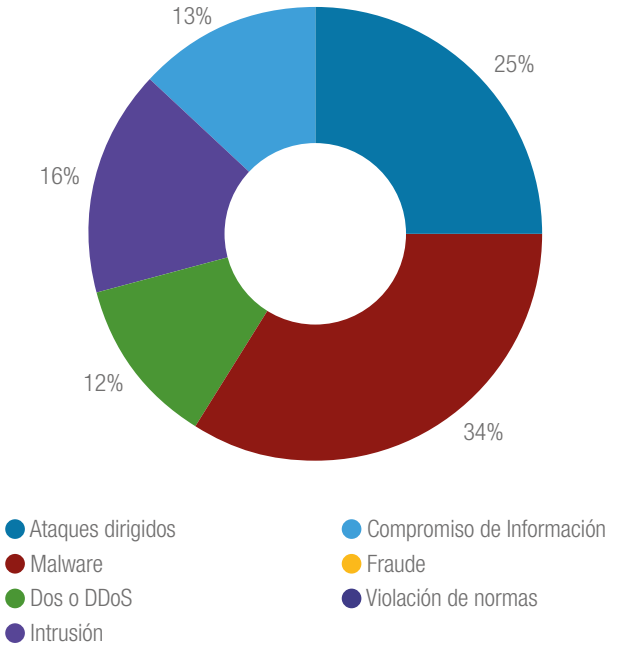


Gráfico 20 – Operadores de servicios esenciales: Incidentes del propio sector.

Sector Eléctrico

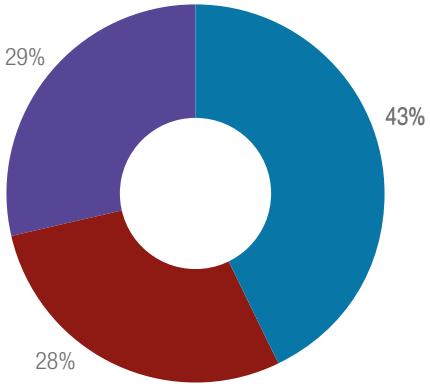


Gráfico 21 – Operadores del sector Eléctrico: Incidentes del propio sector.

Sector Gas y Petróleo

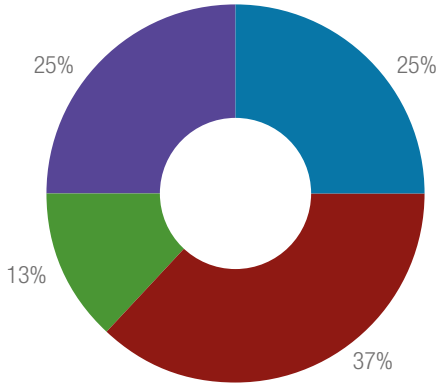


Gráfico 22 – Operadores del sector Gas y Petróleo: Incidentes del propio sector.

Sector Agua

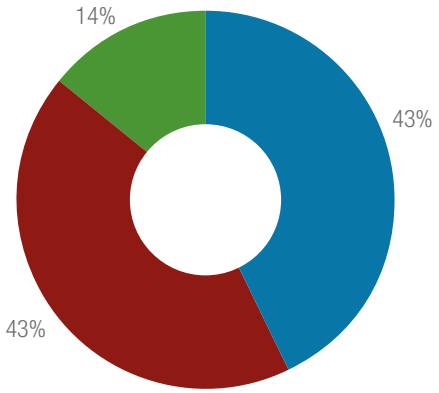


Gráfico 23 – Operadores del sector Agua: Incidentes del propio sector.

Sector Salud

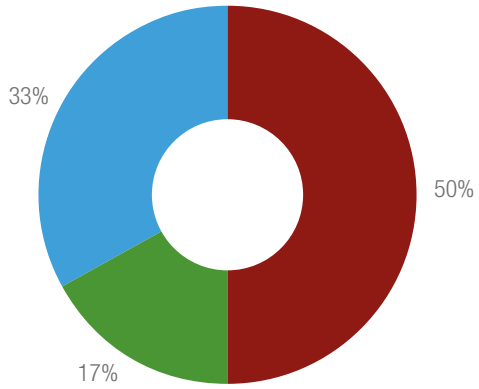


Gráfico 24 – Operadores del sector Salud: Incidentes del propio sector.

Sector Transporte

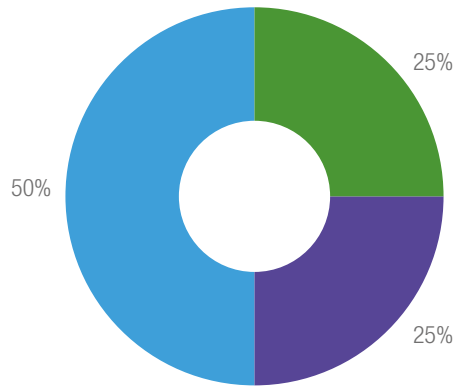


Gráfico 25 – Operadores del sector Transporte: Incidentes del propio sector.

- Ataques dirigidos
- Malware
- Dos o DDoS
- Intrusión
- Compromiso de Información
- Fraude
- Violación de normas

SISTEMAS AFECTADOS POR INCIDENTES EN EL SECTOR

¿Cuáles son los sistemas afectados por incidentes en operadores de su sector que conoce?

Según el 80% de los encuestados los sistemas que suelen verse afectados en los Servicios Esenciales son los sistemas de supervisión y las infraestructuras de comunicaciones.

SISTEMAS AFECTADOS EN SU SECTOR

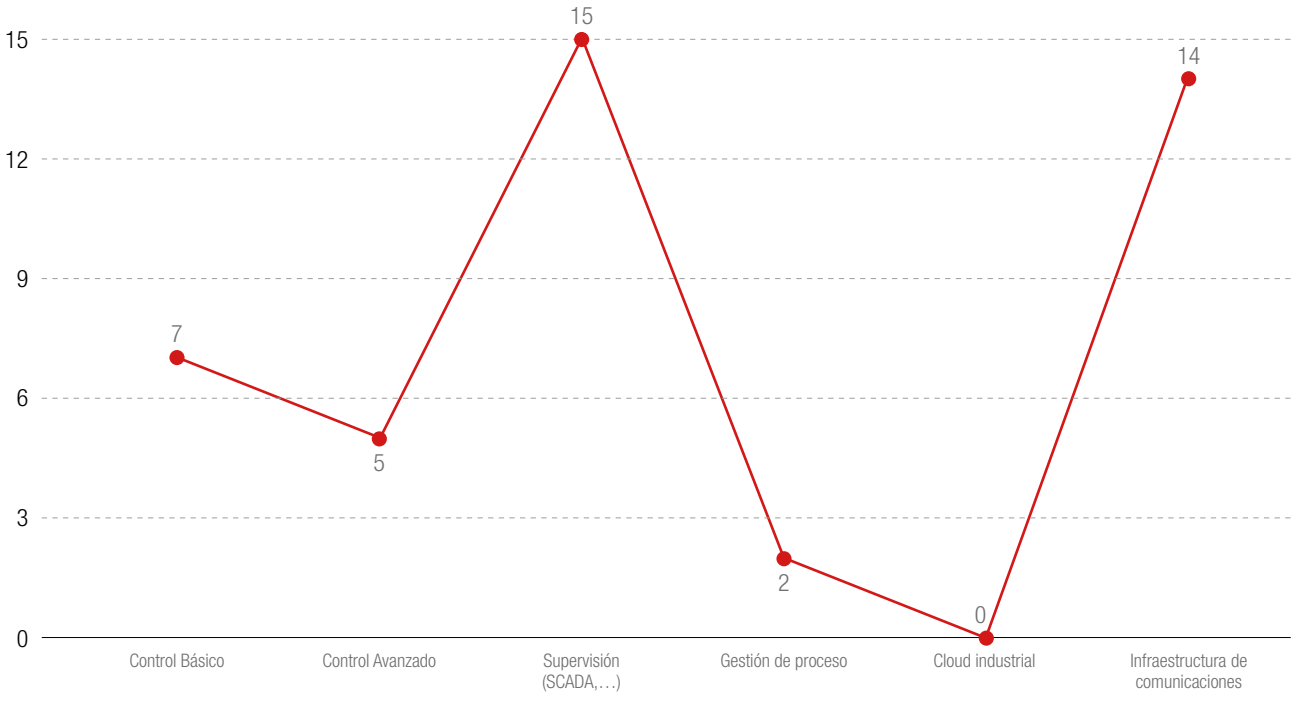


Gráfico 26 – Operadores de servicios esenciales: Sistemas afectados del sector.

Sector Eléctrico

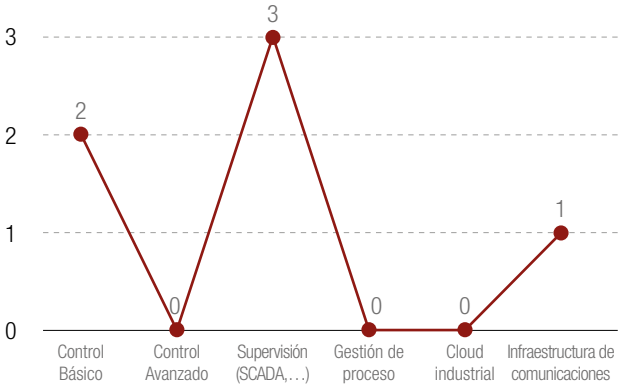


Gráfico 27 – Operadores del sector Eléctrico: Sistemas afectados del sector.

Sector Gas y Petróleo

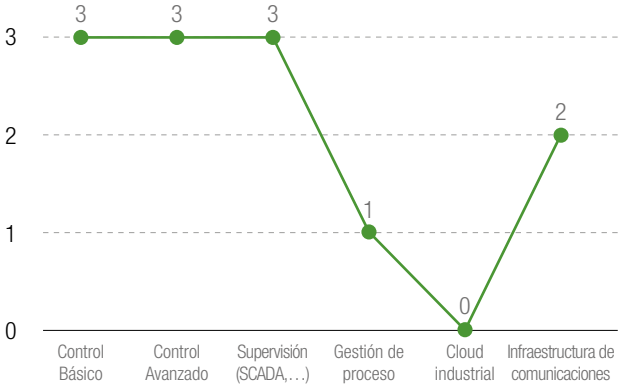


Gráfico 28 – Operadores del sector Gas y Petróleo: Sistemas afectados del sector.

Sector Agua

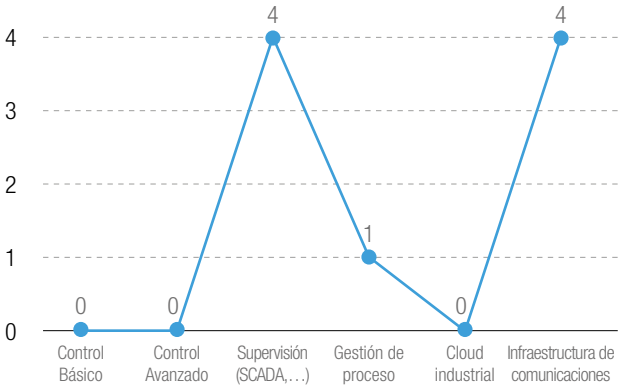


Gráfico 29 – Operadores del sector Agua: Sistemas afectados del sector.

Sector Salud

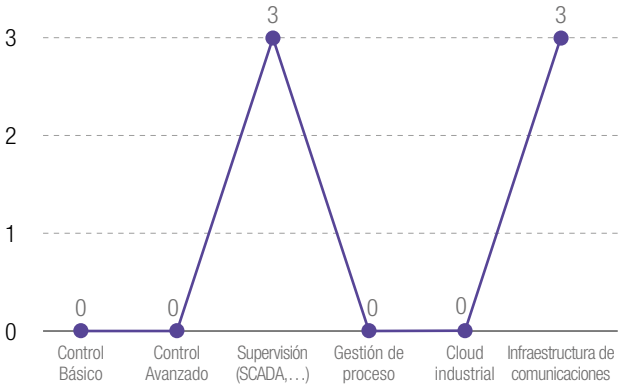


Gráfico 30 – Operadores del sector Salud: Sistemas afectados del sector.

Sector Transporte

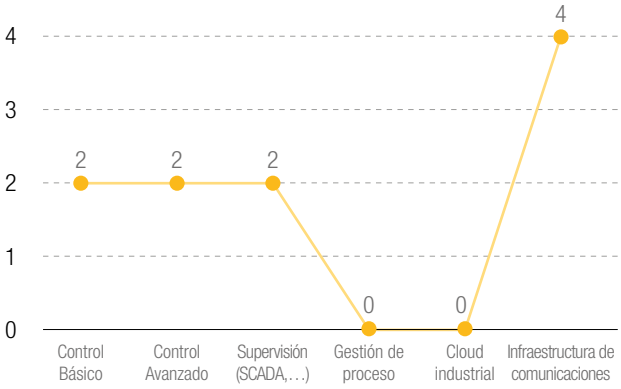


Gráfico 31 – Operadores del sector Transporte: Sistemas afectados del sector.

De las gráficas por sectores se puede destacar que en los sectores eléctrico, oil & gas y transporte, también los sistemas de control suelen verse afectados por incidentes de ciberseguridad.

DEPENDENCIA DE TECNOLOGÍAS DE OPERACIÓN DEL SECTOR

¿Cuál es el grado de dependencia tecnológica en la automatización de procesos en su sector?

Cuando hablamos de tecnologías de automatización industrial, la forma más habitual de presentar estas tecnologías es mediante la pirámide de la siguiente figura.

Nivel 0 – En este nivel encontramos todos los sensores y actuadores que se encuentran repartidos por el proceso, existiendo un control directo de las máquinas y sistemas de producción con muy alta velocidad e intercambia pequeños flujos de datos.

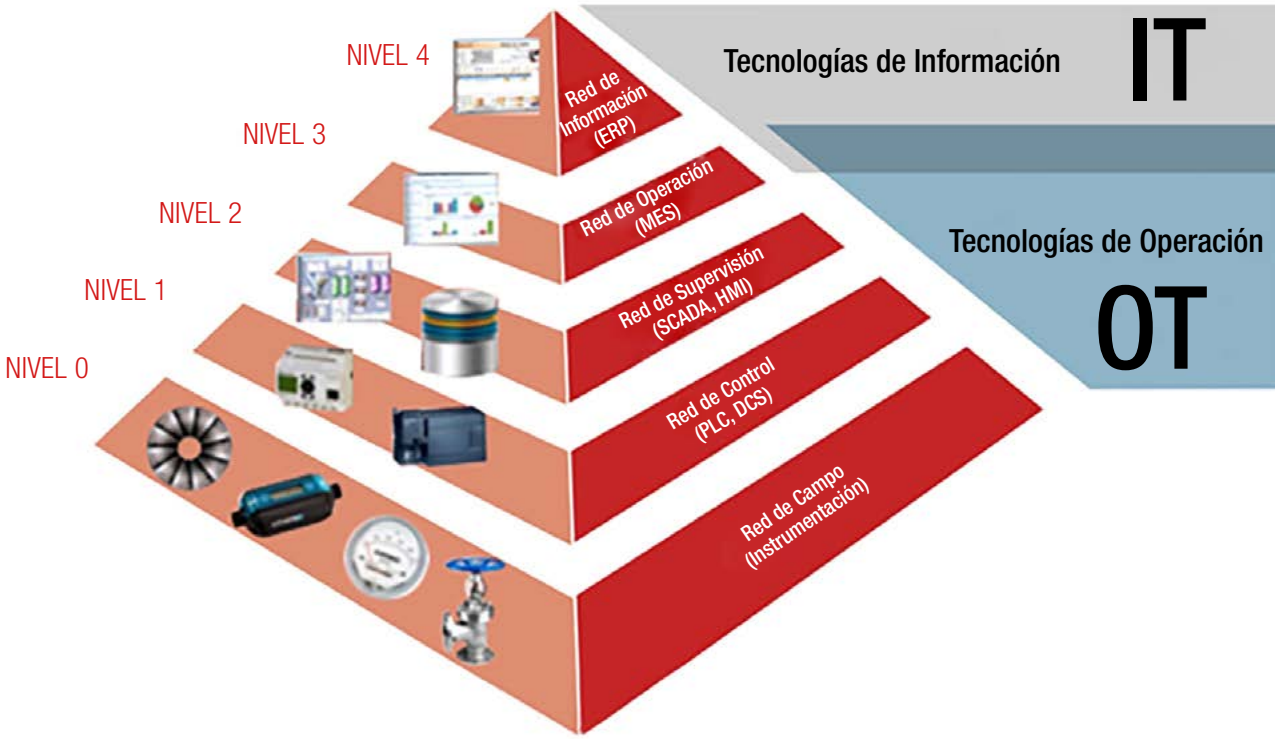
Nivel 1 – En este nivel de control se agrupan todos los instrumentos de control local tales como ordenadores, Controladores lógicos programables (PLCs), etc. Los equipos de este nivel utilizarán datos del proceso proporcionados por los equipos del nivel 0 y darán las consignas a los actuadores y máquinas de dicho nivel.

Nivel 2 – Nivel de supervisión donde se encuentran los equipos destinados a supervisar la secuencia de fabricación y/o producción, como las estaciones de los operadores o el servidor de ingeniería.

Nivel 3 – Nivel de operaciones de optimización de la fabricación donde se gestionan los flujos de trabajo para producir los productos finales. En este nivel existe necesidad de integrar los datos de los niveles inferiores con el nivel superior.

Nivel 4 – Nivel de gestión donde se desarrollan todas las actividades relacionadas con el negocio necesarias en una organización industrial, comunicando distintas plantas y manteniendo relaciones con proveedores y clientes.

El 30% de los entrevistados consideran que la dependencia tecnológica es media a nivel de control y supervisión, y media a nivel de integración. Únicamente el 13% de los entrevistados considera que existe una dependencia alta a todos los niveles.



DEPENDENCIA TECNOLÓGICA

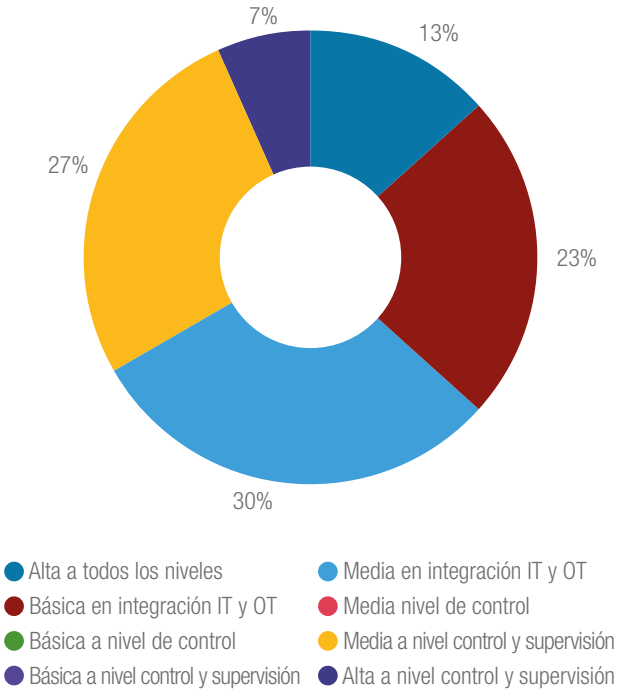


Gráfico 32 – Operadores de Servicios Esenciales: dependencia tecnológica del sector.

Sector Eléctrico

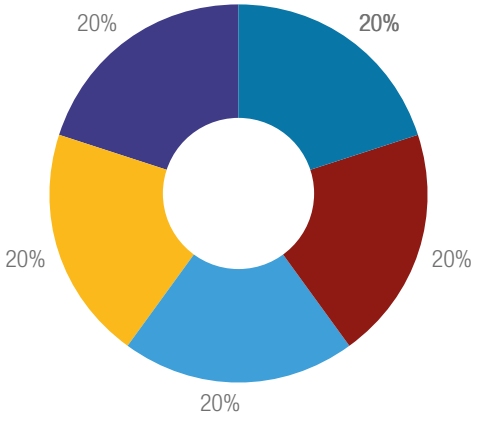


Gráfico 33 – Operadores del sector Eléctrico: dependencia tecnológica del sector.

Sector Gas y Petróleo

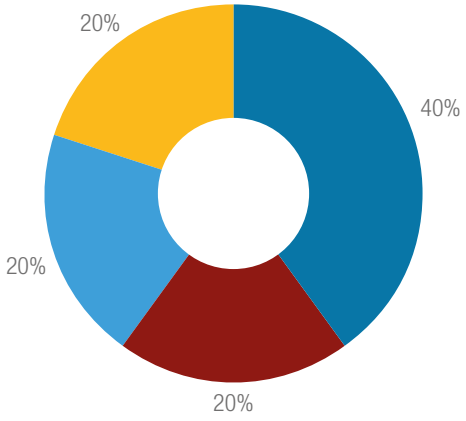


Gráfico 34 – Operadores del sector Gas y Petróleo: dependencia tecnológica del sector..

Sector Agua

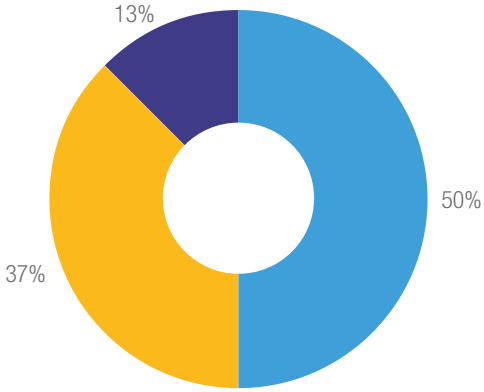


Gráfico 35 – Operadores del sector Agua: dependencia tecnológica del sector.

Sector Salud

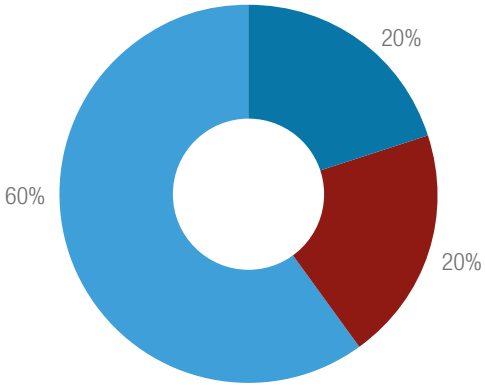


Gráfico 36 – Operadores del sector Salud: dependencia tecnológica del sector.

Sector Transporte

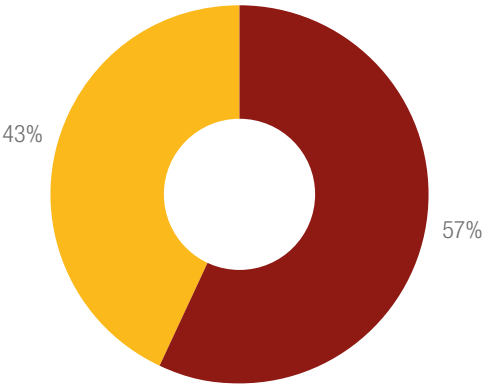


Gráfico 37 – Operadores del sector Transporte: dependencia tecnológica del sector.

De las gráficas sectoriales se puede destacar el sector Gas y Petróleo donde el 40% de los entrevistados considera que la dependencia tecnológica es alta a todos los niveles. Siendo el sector transporte donde se considera que existe un bajo nivel de integración IT y OT.

- Alta a todos los niveles
- Básica en integración IT y OT
- Básica a nivel de control
- Básica a nivel control y supervisión
- Media en integración IT y OT
- Media nivel de control
- Media a nivel control y supervisión
- Alta a nivel control y supervisión

VULNERABILIDADES EN EL SECTOR

¿Cuál considera que es el grado de vulnerabilidades en su sector?

Las tecnologías que se utilizan en la automatización y control industrial son muy diversas. El Equipo de Respuesta a Emergencias Informáticas de Sistemas de Control Industrial (ICS-CERT) perteneciente al gobierno de Estados Unidos, que se ocupa de la seguridad relacionada con los sistemas de control industrial publico en 2015 un informe sobre vulnerabilidades en diferentes sectores, concluyendo que sectores como el energético (eléctrico, gas y petróleo) y el sector agua, tienen más vulnerabilidades que el sector transporte o salud.

GRADO DE VULNERABILIDADES

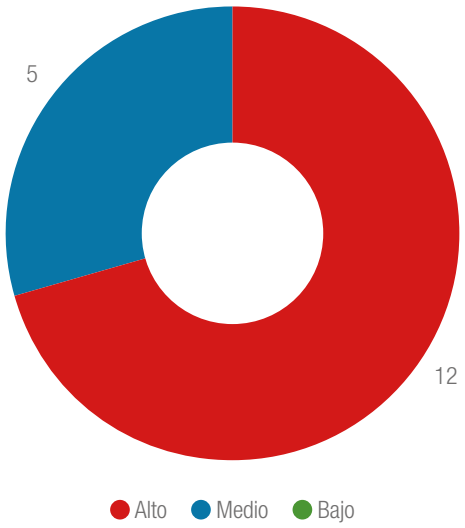


Gráfico 38 – Operadores de Servicios Esenciales: Vulnerabilidades en el sector.

NÚMERO DE VULNERABILIDADES QUE ICS-CERT HA REPORTADO POR SECTOR

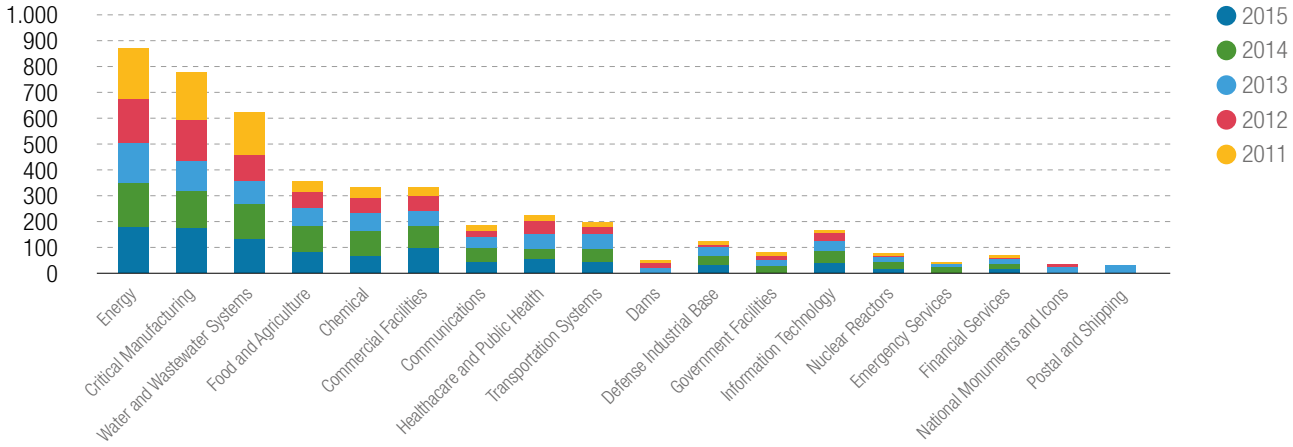


Gráfico 39

La razón principal es que en estos sectores se usan más tecnologías comerciales, que son las tecnologías donde se han descubierto y publicado más vulnerabilidades.

En general casi el 75% de los entrevistados consideran que el nivel de vulnerabilidad de las infraestructuras OT de los servicios esenciales es alto.

Sector Eléctrico

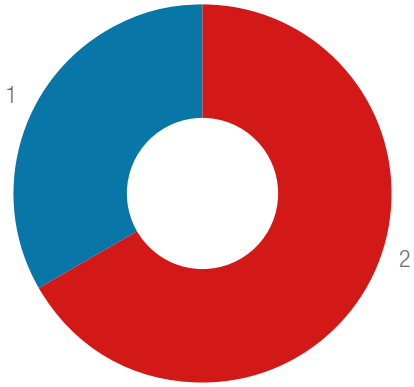


Gráfico 40 – Operadores del sector Eléctrico: Vulnerabilidades en el sector.

Sector Gas y Petróleo

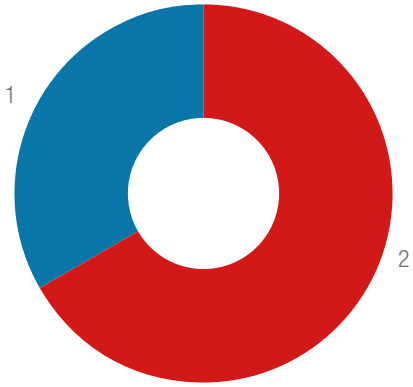


Gráfico 41 – Operadores del sector Gas y Petróleo: Vulnerabilidades en el sector.

Sector Agua

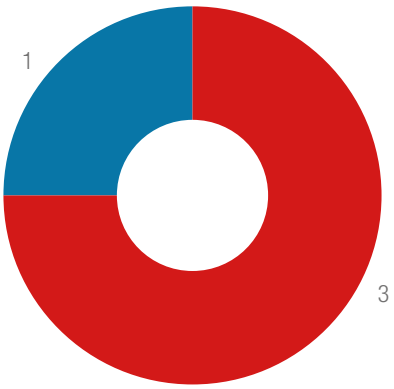


Gráfico 42 – Operadores del sector Agua: Vulnerabilidades en el sector.

Sector Salud

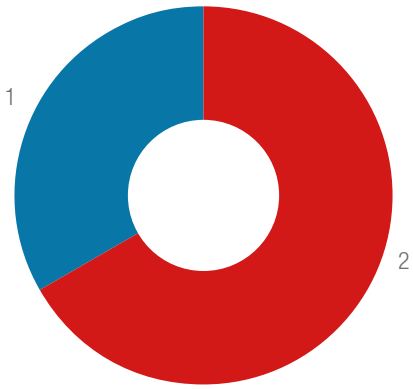


Gráfico 43 – Operadores del sector Salud: Vulnerabilidades en el sector.

Sector Transporte

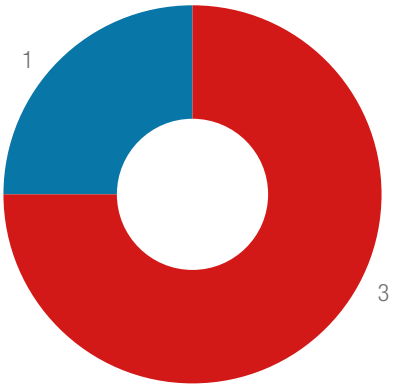


Gráfico 44 – Operadores del sector Transporte: Vulnerabilidades en el sector.

Alto Medio Bajo

CONSECUENCIAS DE INCIDENTES EN EL SECTOR

¿Cuáles considera que son las consecuencias de los incidentes en su sector?

Casi un 30% de los profesionales encuestados consideran que la perdida de un servicio esencial es una de las principales consecuencias de los incidentes de ciberseguridad. Esto es debido principalmente a que las tecnologías industriales que operan servicios esenciales no han incorporado requisitos de ciberseguridad lo cual les hace muy vulnerables frente a comportamientos no esperados.

CONSECUENCIAS DE LOS INCIDENTES

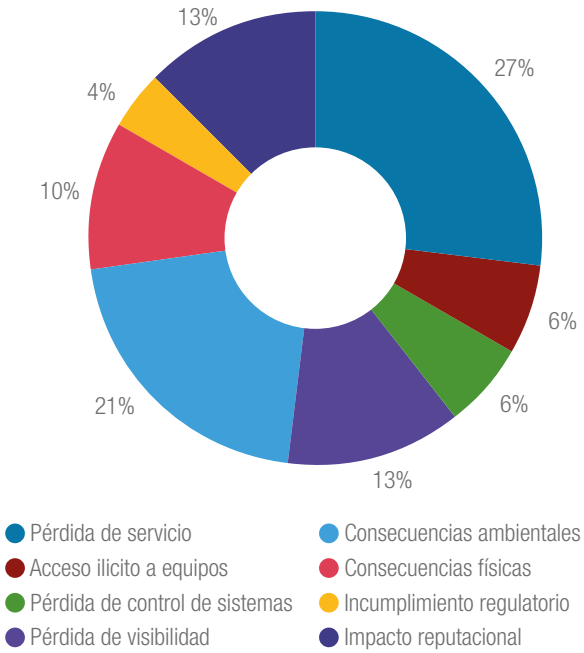


Gráfico 45 – Operadores de Servicios Esenciales: Consecuencias de incidentes en el sector.

Sector Eléctrico

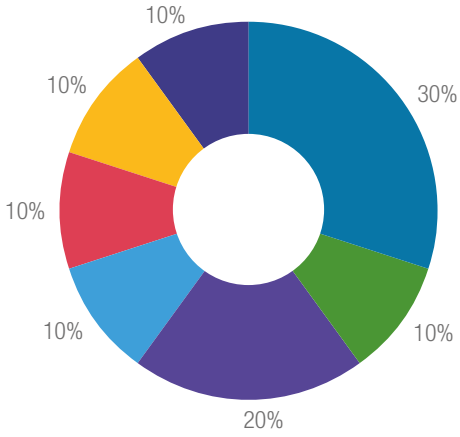


Gráfico 46 – Operadores del sector Eléctrico: Consecuencias de incidentes en el sector.

Sector Gas y Petróleo

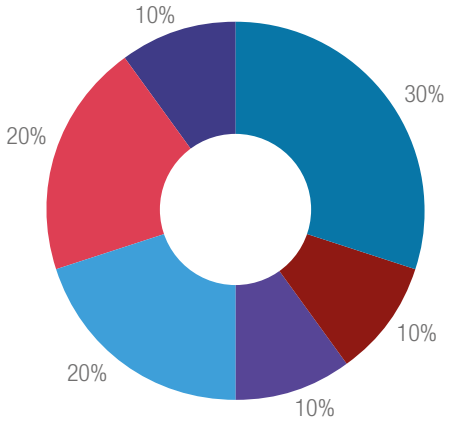


Gráfico 47 – Operadores del sector Gas y Petróleo: Consecuencias de incidentes en el sector.

Sector Agua

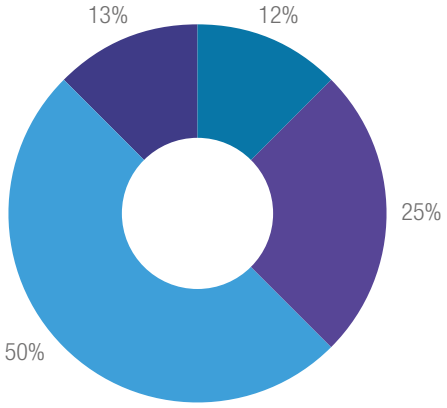


Gráfico 48 – Operadores del sector Agua: Consecuencias de incidentes en el sector.

Sector Salud

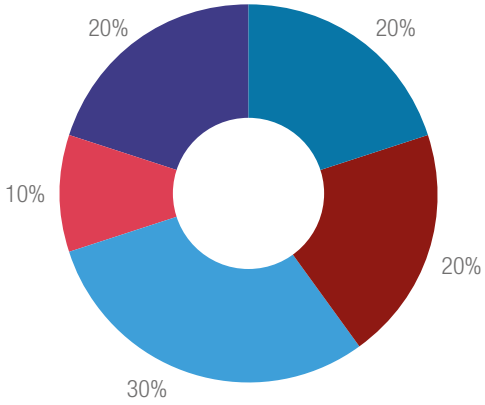


Gráfico 49 – Operadores del sector Salud: Consecuencias de incidentes en el sector.

Sector Transporte

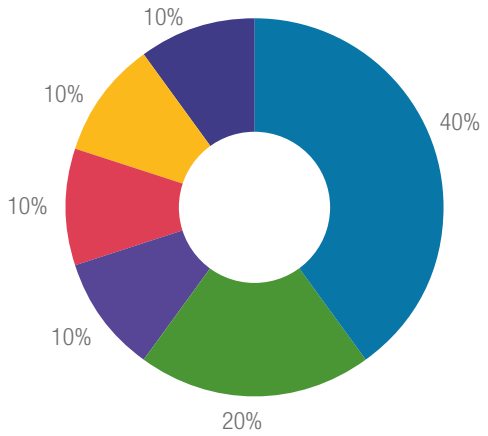


Gráfico 50 – Operadores del sector Transporte: Consecuencias de incidentes en el sector.

- Pérdida de servicio
- Acceso ilicito a equipos
- Pérdida de control de sistemas
- Pérdida de visibilidad
- Consecuencias ambientales
- Consecuencias físicas
- Incumplimiento regulatorio
- Impacto reputacional

ESTRUCTURA PARA GESTIONAR INCIDENTES

¿Cuál es la estructura de su organización para gestionar los incidentes de ciberseguridad OT?

El elemento más importante de un SOC son las personas. Un SOC es un equipo compuesto principalmente por especialistas tecnológicos, analistas, ingenieros de seguridad y profesionales de inteligencia que estarán organizados para detectar, analizar, responder, informar y prevenir incidentes de ciberseguridad.

Los SOC pueden variar desde pequeños centros de cinco personas, hasta grandes centros nacionales de coordinación. La estructura y tamaño del SOC debe corresponderse con su alcance equilibrando tres necesidades:

- Tener un equipo cohesionado de especialistas en seguridad o equipos adecuadamente coordinados.
- Mantener la proximidad lógica, física y organizacional a los activos que se monitorizan.
- Disponer de un presupuesto previamente aprobado por la Alta Dirección; acorde al tipo de negocio, servicio o infraestructura crítica soportada.

Según la gráfica general no existe actualmente una estructura dominante en un SOC para gestionar incidentes, la mitad de los encuestados han indicado que la gestión es propia y la otra mitad que la gestión es externa. Tampoco existe una respuesta determinante entre gestión IT y OT integrada o independiente, siendo ligeramente en más casos la gestión independiente.

ESTRUCTURA ORGANIZATIVA EN LA GESTIÓN DE INCIDENTES

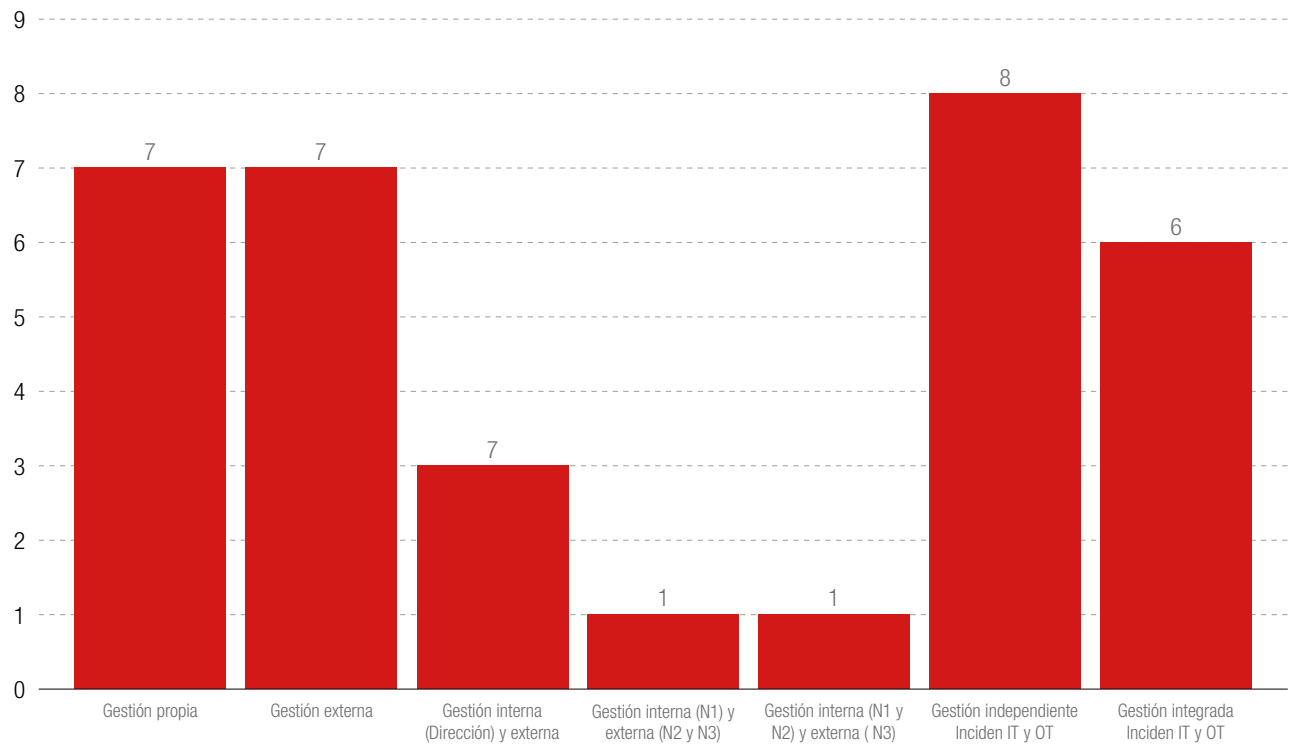


Gráfico 51 – Operadores de Servicios Esenciales: Estructura para gestionar incidentes.

Sector Eléctrico

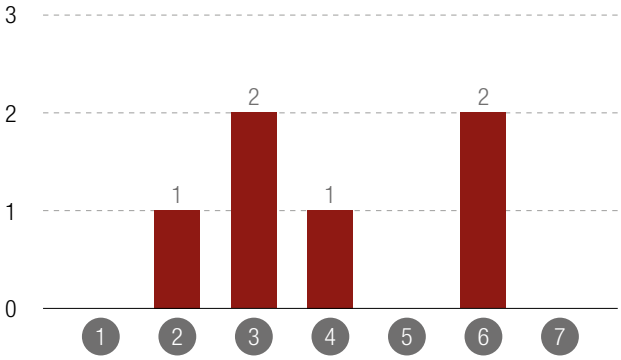


Gráfico 52 – Operadores del sector Eléctrico: Estructura para gestionar incidentes.

Sector Gas y Petróleo

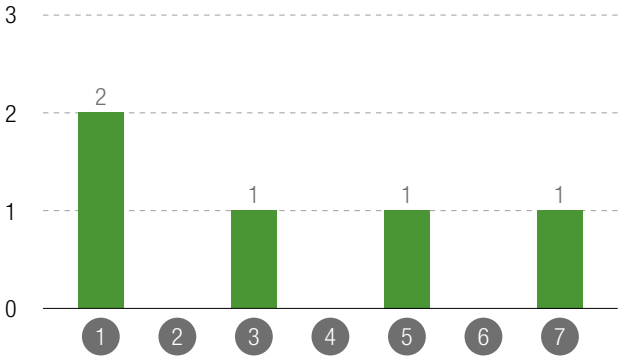


Gráfico 53 – Operadores del sector Gas y Petróleo: Estructura para gestionar incidentes.

Sector Agua

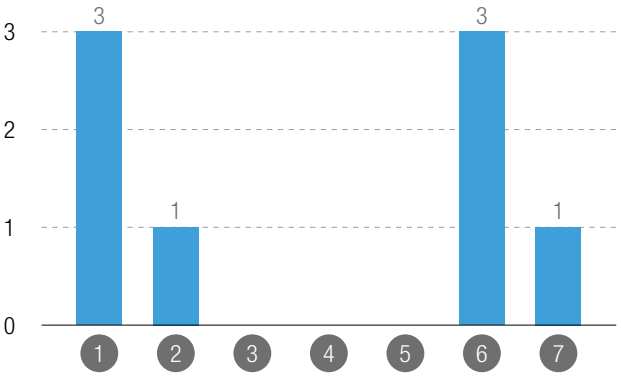


Gráfico 54 – Operadores del sector Agua: Estructura para gestionar incidentes.

Sector Salud

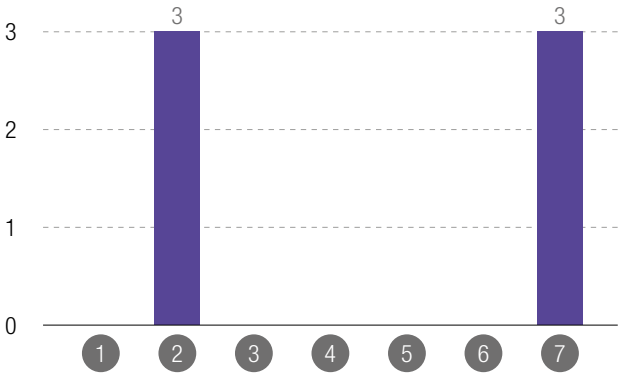


Gráfico 55 – Operadores del sector Salud: Estructura para gestionar incidentes.

Sector Transporte

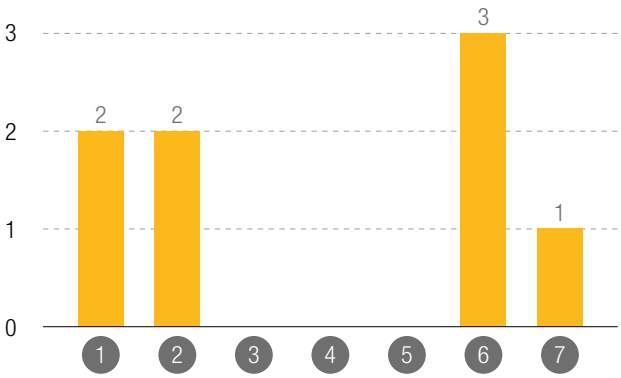


Gráfico 56 – Operadores del sector Transporte: Estructura para gestionar incidentes.

Analizando los datos de forma sectorizada podemos comprobar que los sectores gas y petróleo, agua y transporte tienen claramente una gestión propia, mientras que el sector eléctrico y salud tienen gestión externa.

1. Gestión propia
2. Gestión externa
3. Gestión interna (Dirección) y externa
4. Gestión interna (N1) y externa (N2 y N3)
5. Gestión interna (N1 y N2) y externa (N3)
6. Gestión independiente Inciden IT y OT
7. Gestión integrada Inciden IT y OT

RELACIÓN CON ENTIDADES EXTERIORES EN LA GESTIÓN DE INCIDENTES

¿Cuál es su relación con entidades exteriores para reducir el impacto de los incidentes OT?

Es significativo comprobar que actualmente existe una escasa relación con las entidades CSIRT nacionales (32%), lo que indica que aún no se han establecido los canales de comunicación necesarios para la notificación de incidentes, tal y como se establece en el real decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información donde se promulga la gestión de incidentes de ciberseguridad como una imposición legal para todas las organizaciones públicas y algunas privadas de España que prestan servicios esenciales.

RELACIÓN CON ENTIDADES

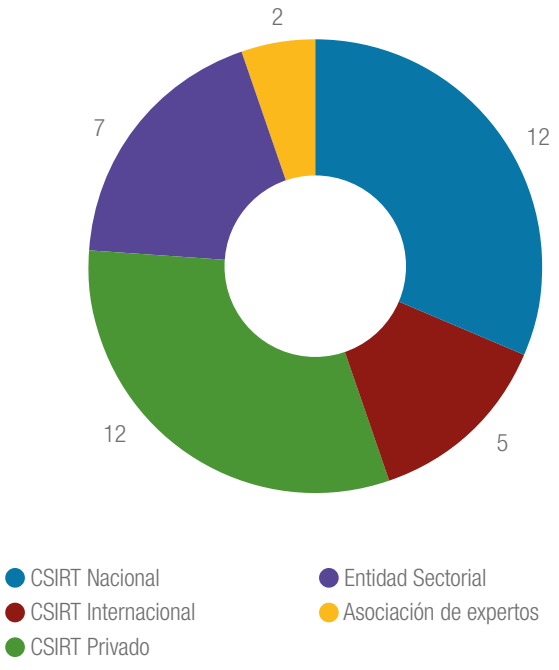


Gráfico 57 – Operadores Servicios Esenciales: Relación con entidades exteriores.

Sector Eléctrico

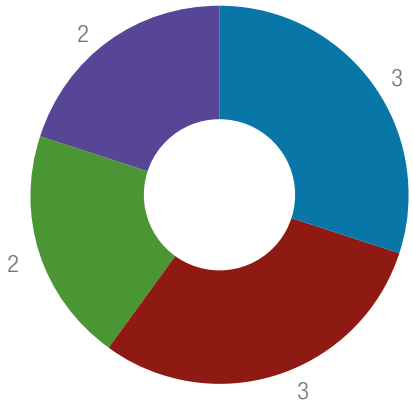


Gráfico 58 – Operadores del sector Eléctrico: Relación con entidades.

Sector Gas y Petróleo

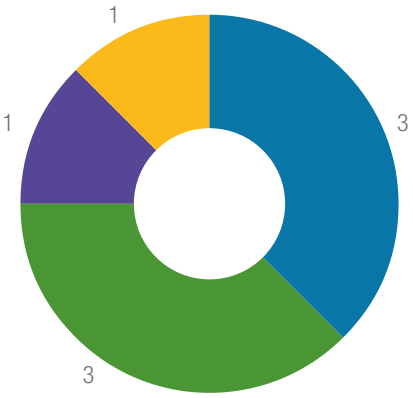


Gráfico 59 – Operadores del sector Gas y Petróleo: Relación con entidades.

Sector Agua

Gráfico 60 – Operadores del sector Agua: Relación con entidades.

Sector Salud

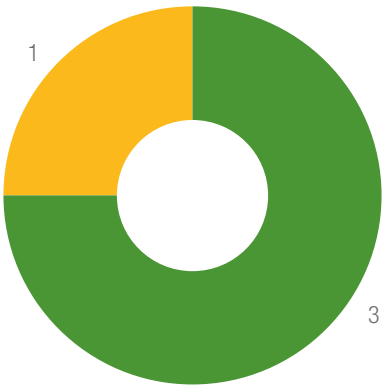


Gráfico 61 – Operadores del sector Salud: Relación con entidades.

Sector Transporte

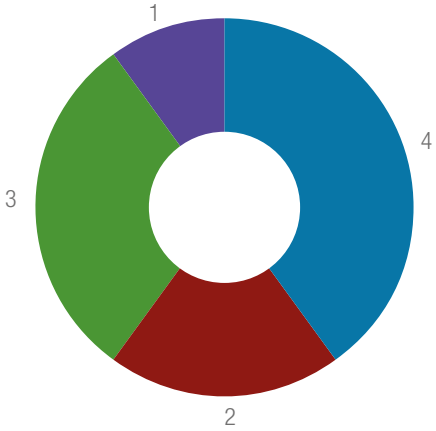


Gráfico 62 – Operadores del sector Transporte: Relación con entidades.

CAPACIDADES PARA DAR RESPUESTA A INCIDENTES

¿Qué capacidades tiene su organización para dar respuesta a incidentes de alto impacto en la operación de servicios esenciales?

Según este estudio, al preguntar sobre las capacidades de respuesta distinguiendo entre tecnologías de información (IT) y tecnologías de operación (OT) se ve claramente que las capacidades de respuesta en entornos IT es alta según un 50% de los encuestados, lo que contrasta con el un 20% de capacidad de respuesta en un entorno OT. Es cierto, que actualmente las organizaciones que han participado en la encuesta están inmersas en un proceso de adecuación de su SOC para gestionar incidentes, lo cual indica que un alto porcentaje de organizaciones industriales están gestionando o empezando a gestionar los riesgos tecnológicos.

CAPACIDADES DE RESPUESTA

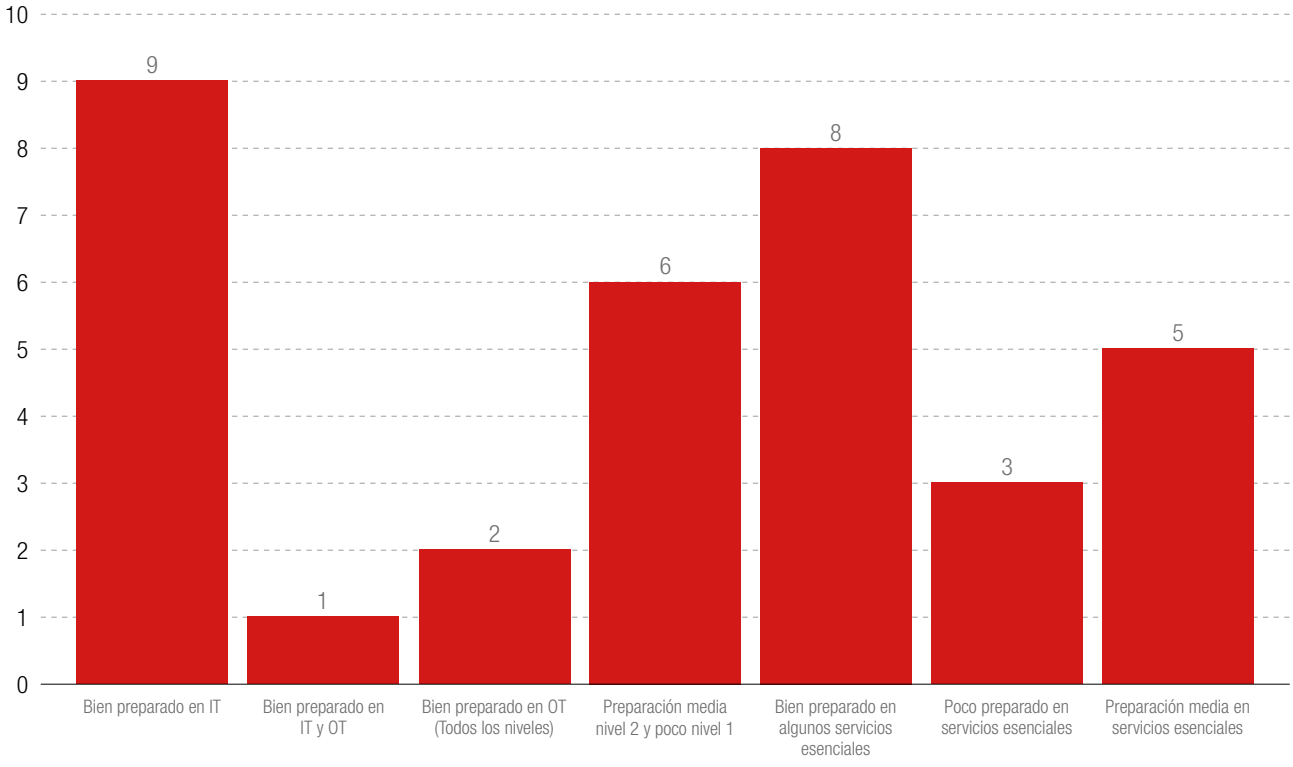


Gráfico 63 – Operadores de Servicios Esenciales: Capacidades de respuesta a incidentes.

Sector Eléctrico

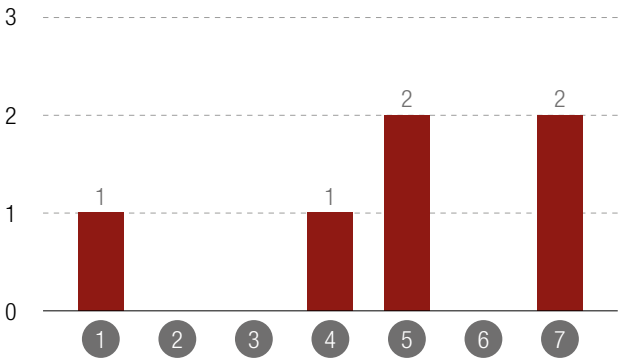


Gráfico 64 – Operadores del sector Eléctrico: Capacidades de respuesta a incidentes.

Sector Gas y Petróleo

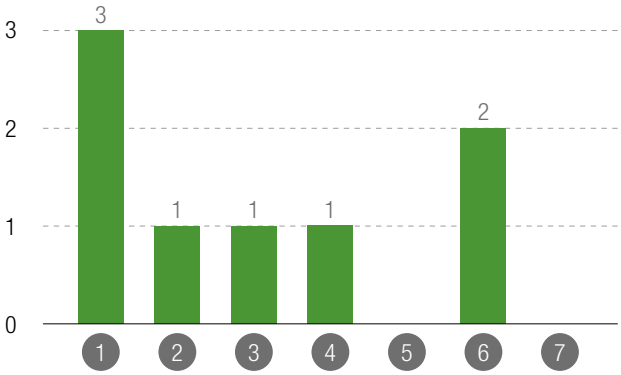


Gráfico 65 – Operadores del sector Gas y Petróleo: Capacidades de respuesta a incidentes.

Sector Agua

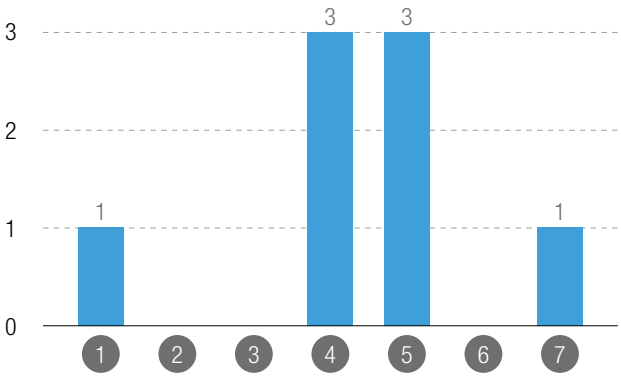


Gráfico 66 – Operadores del sector Agua: Capacidades de respuesta a incidentes.

Sector Salud

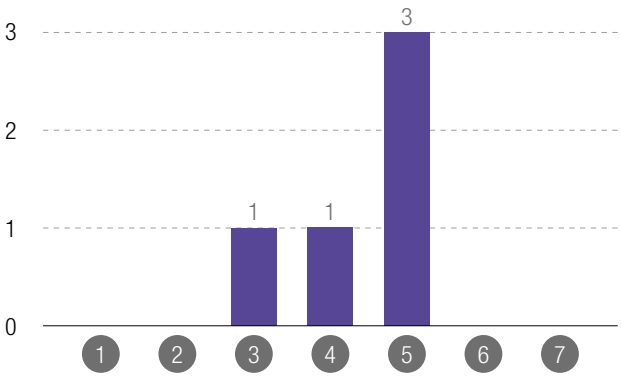


Gráfico 67 – Operadores del sector Salud: Capacidades de respuesta a incidentes.

Sector Transporte

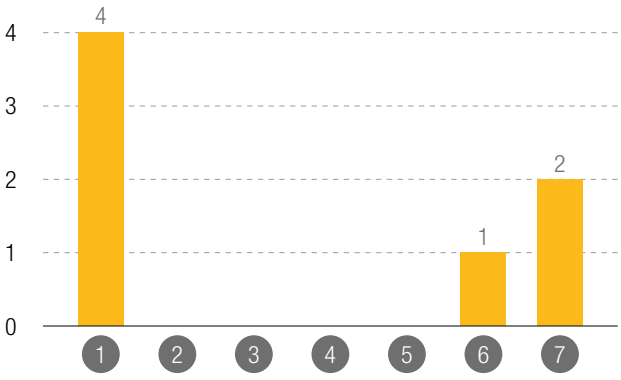


Gráfico 68 – Operadores del sector Transporte: Capacidades de respuesta a incidentes.

1. Bien preparado en IT
2. Bien preparado en IT y OT
3. Bien preparado en OT (Todos los niveles)
4. Preparación media nivel 2 y poco nivel 1
5. Bien preparado en algunos servicios esenciales
6. Poco preparado en servicios esenciales
7. Preparación media en servicios esenciales

PARTICIPACIÓN DE DISTINTAS ÁREAS DE LA ORGANIZACIÓN

¿Como participan las distintas áreas de la organización en los aspectos de ciberseguridad (Calidad, HSE, …)?

La responsabilidad de proteger los sistemas de control industrial sigue recayendo de manera muy nítida en el área de TI corporativa -sigue contemplándose la responsabilidad de estos riesgos en el área tecnológica-.

La participación de otras áreas, como Calidad, Compras, HSE, es de momento muy baja, aumentando levemente (33%) solo cuando se trata de proyectos estratégicos, lo que podemos interpretar, que continúa existiendo una falta clara de madurez organizativa en las compañías en las que la asignación de responsabilidades no se hace atendiendo a un proceso formal y definido, sino que se atiende a meros aspectos regulatorios, al historial de la organización, al carisma de los interesados o, en el mejor de los casos, a las necesidades reales, fruto de un análisis de las actuales amenazas, todo lo cual suele terminar polarizando las responsabilidades en ciertos departamentos.

Otra de las causas posibles, y que durante los últimos meses hemos podido constatar a través de entrevistas con responsables de organizaciones industriales es la falta de conocimiento y concienciación de la Dirección, que frecuentemente asigna cualquier tema relacionado con las redes de comunicaciones industriales y su seguridad a los departamentos de TI, sin entender que aunque se emplee tecnología similar, su aplicación es a un entorno industrial muy heterogéneo donde las consecuencias, los requerimientos y sus características son muy diferentes.

PARTICIPACIÓN OTRAS ÁREAS

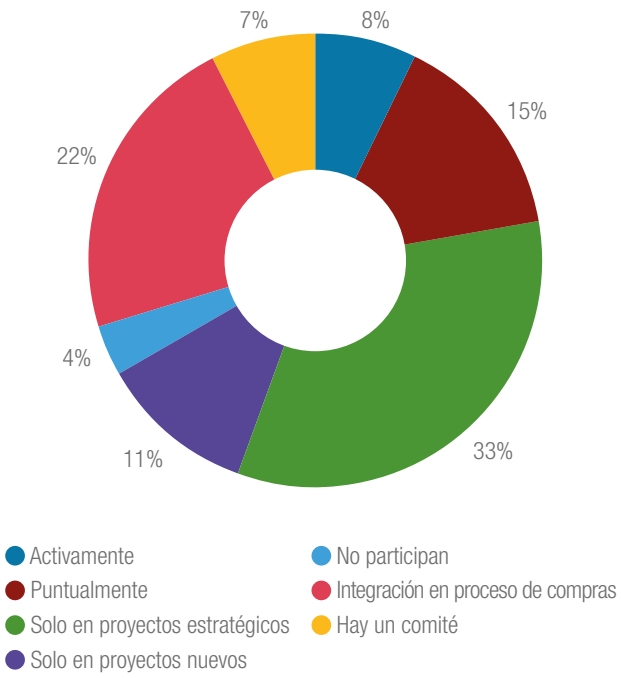


Gráfico 69 – Operadores de Servicios Esenciales: Participación de áreas de la organización.

Sector Eléctrico

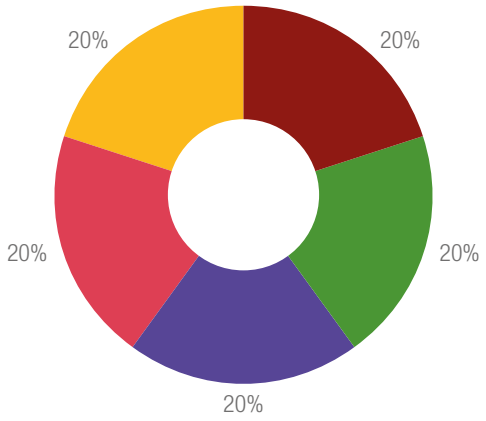


Gráfico 70 – Operadores del sector eléctrico: Participación de áreas de la organización.

Sector Gas y Petróleo

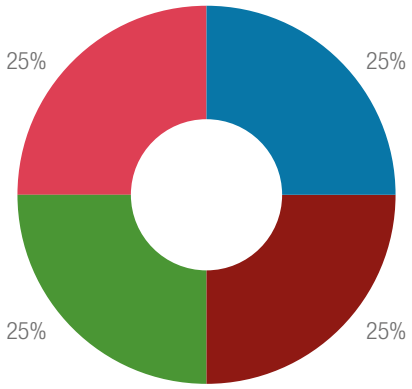


Gráfico 71 – Operadores del sector Gas y Petróleo: Participación de áreas de la organización.

Sector Agua

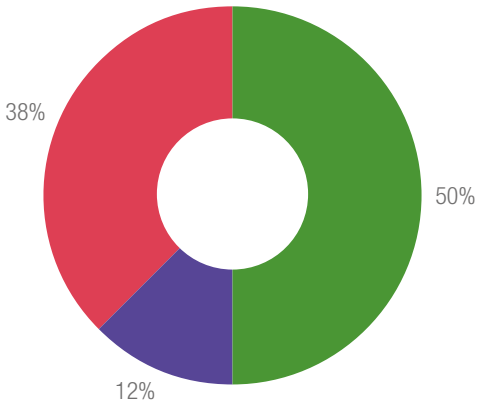


Gráfico 72 – Operadores del sector Agua: Participación de áreas de la organización.

Sector Salud

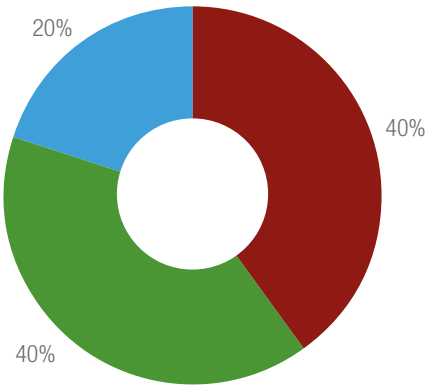


Gráfico 73 – Operadores del sector Salud: Participación de áreas de la organización.

Sector Transporte

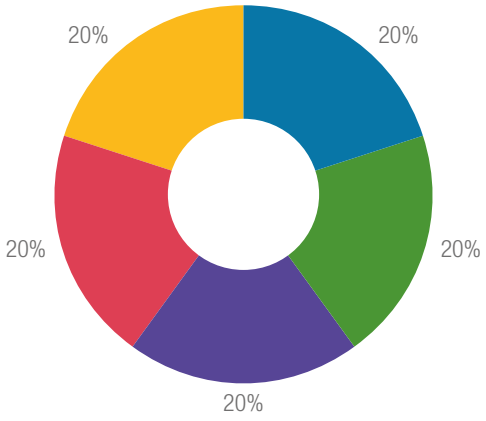


Gráfico 74 – Operadores del sector Transporte: Participación de áreas de la organización.

- Activamente
- Puntualmente
- Solo en proyectos estratégicos
- Solo en proyectos nuevos
- No participan
- Integración en proceso de compras
- Hay un comité

PETICIÓN Y EVALUACIÓN DE REQUISITOS DE CIBERSEGURIDAD

¿Cómo se realiza la petición y evaluación de requisitos de ciberseguridad en nuevos proyectos para servicios esenciales que presta su organización?

La mayoría de las organizaciones industriales empiezan a contemplar, al menos, requisitos básicos de Ciberseguridad Industrial en sus nuevos proyectos. Siendo los correspondientes a las infraestructuras de comunicaciones donde se contempla mayor exigencia, tanto en las redes WAN (conexiones y accesos a redes remotas) y LAN (redes locales).

PETICIÓN DE REQUISITOS DE CIBERSEGURIDAD

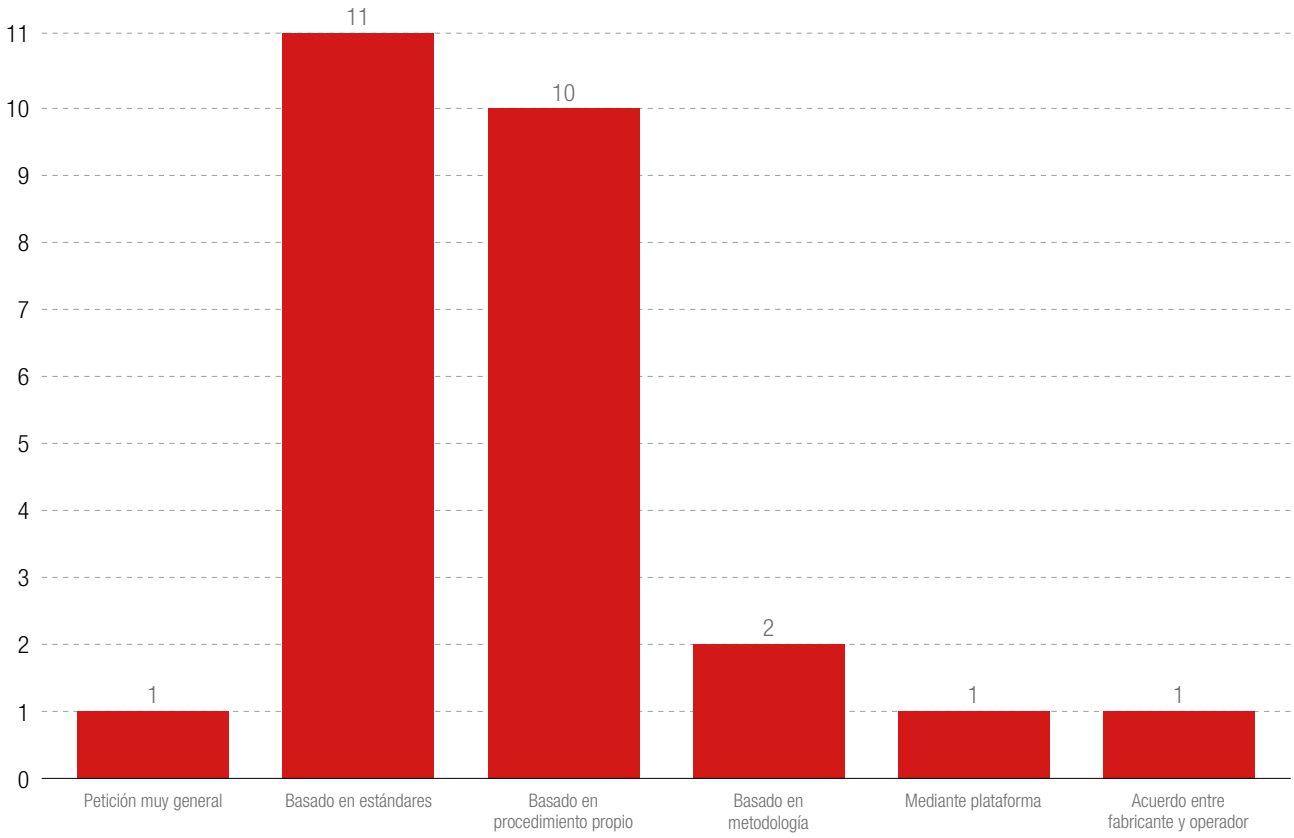


Gráfico 75 – Operadores de Servicios Esenciales: Petición de requisitos de ciberseguridad.

Sector Eléctrico

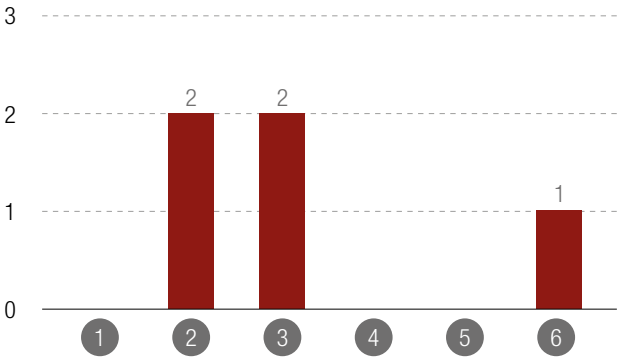


Gráfico 76 – Operadores del sector Eléctrico: Petición requisitos ciberseguridad.

Sector Gas y Petróleo

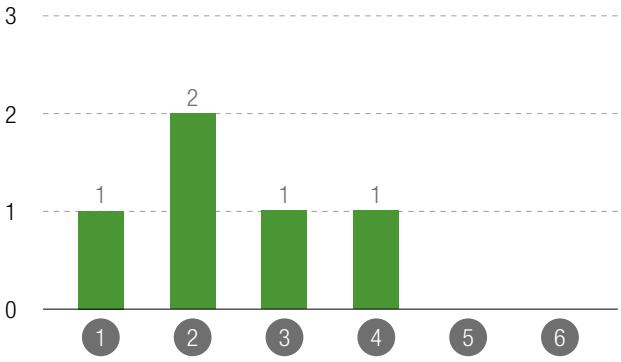


Gráfico 77 – Operadores del sector Gas y Petróleo: Petición requisitos ciberseguridad.

Sector Agua

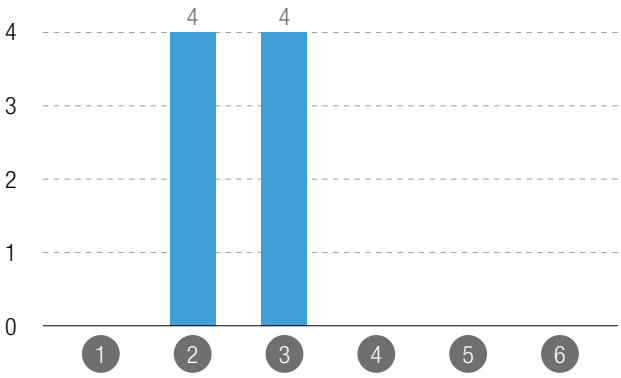


Gráfico 78 – Operadores del sector Agua: Petición requisitos ciberseguridad.

Sector Salud

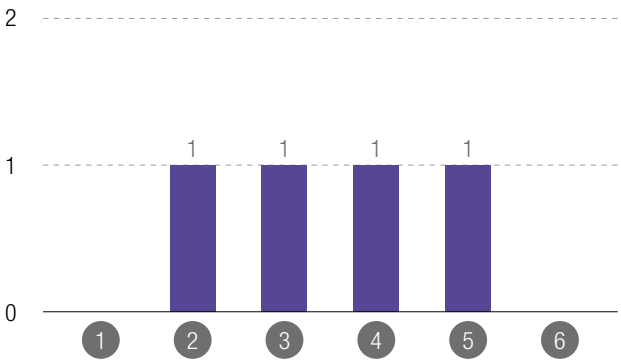


Gráfico 79 – Operadores del sector Salud: Petición requisitos ciberseguridad.

Sector Transporte

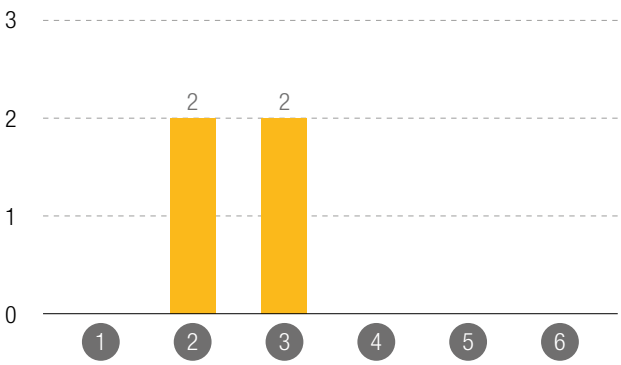


Gráfico 80 – Operadores del sector Transporte: Petición requisitos ciberseguridad.

1. Petición muy general
2. Basado en estándares
3. Basado en procedimiento propio
4. Basado en metodología
5. Mediante plataforma
6. Acuerdo entre fabricante y operador

Como muestra la estadística anterior, a la hora de contemplar requisitos de ciberseguridad en los proyectos de automatización y control de servicios esenciales, estos se basan en estándares y procedimientos propios. Pero hasta el momento, salvo algunas excepciones, las organizaciones que prestan servicios esenciales no tienen una herramienta que permita incorporar los requisitos de ciberseguridad en los proyectos de automatización industrial de forma ordenada, ni tampoco mecanismos adecuados para comprobar las capacidades de los proveedores en estos proyectos.

CONCLUSIONES

La prestación de los servicios esenciales en España está cada vez más ligada a las redes y sistemas de información por el tratamiento tan intenso de los datos (personales o no) y por la creciente automatización de los procesos internos de producción y gestión económica. Ello implica, a su vez, una mayor exposición a los riesgos que existen en el empleo de una red abierta y global, como Internet, canal por el cual también se difunden infecciones de virus y programas maliciosos que pueden llegar a interferir en la prestación de servicios esenciales, provocar fugas de datos personales, comprometer información confidencial de valor comercial y afectar, en fin, al funcionamiento de dicho mercado interior. Como se demuestra en este estudio y en las estadísticas de los CERTs españoles, donde el número de incidentes gestionados ha ido en aumento en los últimos años.

La Directiva NIS impone a las entidades gestoras de servicios esenciales, así como a los prestadores de ciertos servicios digitales considerados clave en el funcionamiento de Internet, la obligación de establecer sistemas de gestión de la seguridad de la información en sus organizaciones y de notificar a las autoridades los incidentes que tengan especial gravedad. Así mismo, obliga a los Estados miembros a dotarse de los medios para supervisar el cumplimiento de estas obligaciones y a velar por que existan equipos de respuesta a incidentes de seguridad con capacidad para proteger a las empresas de la propagación de estos incidentes.

Un incidente de seguridad puede ser visto como un fracaso, puesto que la medida para responder a la amenaza no era adecuada o ni siquiera se había contemplado. Además, un incidente se puede convertir en un fracaso si no lo analizamos y aprendemos para evitar que vuelva a suceder, pero sobre todo si no nos preparamos para reducir sus consecuencias.

Este estudio demuestra que todavía las organizaciones que operan servicios esenciales no están suficientemente preparadas para dar respuesta a los incidentes de ciberseguridad, pero están haciendo grandes esfuerzos por mejorar sus capacidades.

Paseo de las Delicias, 30 · 2º piso
28045 MADRID
+34 910 910 751
info@CCI-es.org
www.CCI-es.org
blog.CCI-es.org
@info_CCI