

CENTRO DE
CIBERSEGURIDAD
INDUSTRIAL



Estudio sobre el estado de la Ciberseguridad Industrial en Euskadi

BASQUE
CYBER
SECURITY
CENTRE


BASQUE
CYBER**SECURITY**
CENTRE

EDICIÓN 2018

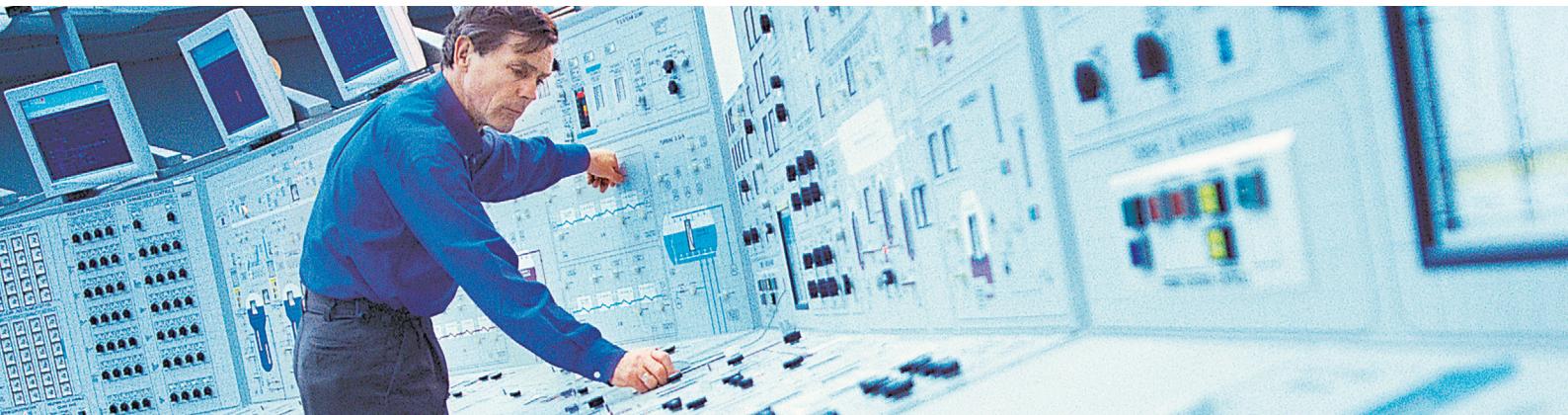
CENTRO DE CIBERSEGURIDAD INDUSTRIAL



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, en un contexto en el que las organizaciones de sectores como el de fabricación o el energético juegan un papel crítico en la construcción de la sociedad actual, como puentes del estado del bienestar.

El CCI afronta ese reto mediante el desarrollo de actividades de investigación y análisis, generación de opinión, elaboración y publicación de estudios y herramientas, e intercambio de información y conocimiento, sobre la influencia, tanto de las tecnologías, incluidos sus procesos y prácticas, como de los individuos, en lo relativo a los riesgos -y su gestión- derivados de la integración de los procesos e infraestructuras industriales en el Ciberespacio.

CCI es, hoy, el ecosistema y el punto de encuentro de las entidades -privadas y públicas- y de los profesionales afectados, preocupados u ocupados de la Ciberseguridad Industrial; y es, asimismo, la referencia hispanohablante para el intercambio de experiencias y la dinamización de los sectores involucrados en este ámbito.



ISBN: 978-84-947727-1-9

Primera edición: octubre de 2018

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra queda rigurosamente prohibida y estará sometida a las sanciones establecidas por la ley. Solamente el autor (Centro de Ciberseguridad Industrial, www.CCI-es.org), puede autorizar la fotocopia o el escaneado de algún fragmento a las personas que estén interesadas en ello.

- 📍 Maiquez, 18 · 28009 MADRID
- 📞 +34 910 910 751
- ✉️ info@CCI-es.org
- 🌐 www.CCI-es.org
- 🌐 blog.CCI-es.org
- 🐦 [@info_CCI](https://twitter.com/info_CCI)
- 🔗 www.linkedin.com/in/centrociberseguridadindustrial/

BASQUE CYBERSECURITY CENTRE



El BASQUE CYBERSECURITY CENTRE (en adelante, BCSC), es una iniciativa que se enmarca en la SOCIEDAD PARA LA TRANSFORMACIÓN COMPETITIVA-ERALDAKETA LEHIAKORRERARO SOZIETATEA, S.A. (en adelante Grupo SPRI), sociedad dependiente del Departamento de Desarrollo Económico e Infraestructuras del Gobierno Vasco. El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

El BCSC es un instrumento del Gobierno Vasco para elevar la cultura de la ciberseguridad en la sociedad vasca y aspira a erigirse como punto de encuentro entre oferentes y demandantes de servicios especializados, generando con ello una oportunidad para la innovación, potenciando la competitividad de las empresas y facilitando que la ciudadanía desarrolle hábitos para una actividad digital más segura.

Para alcanzar sus objetivos, el BCSC se define como una iniciativa transversal que desde su inicio involucra a cuatro Departamentos del Gobierno Vasco, el ya antes citado de Desarrollo Económico e Infraestructuras, el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación.

La actividad del centro incluye proyectos de investigación, iniciativas de emprendimiento y colaboración coordinada con otros agentes competentes a nivel estatal e internacional. No en vano se trabaja en estrecha colaboración con agentes de la Red Vasca de Ciencia Tecnología e Innovación que forman parte de su Comité Permanente.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de la innovación tecnológica, de la investigación y de la transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

El BCSC ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CSIRT, por sus siglas en inglés "Computer Security Incident Response Team") y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar su capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca.

autores

Susana Asensio

Javier Diéguez

Edorta Echave

Asier Martínez

José Valiente

índice

00.	
INTRODUCCIÓN	6
Descripción del estudio	8
Sectores analizados	8
Agradecimientos	8
01.	
ORGANIZACIÓN DE LA CIBERSEGURIDAD INDUSTRIAL	11
Responsabilidad respecto a la ciberseguridad industrial	13
Grado de capacitación en ciberseguridad industrial	15
02.	
GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL	17
Evaluación de riesgos	19
Gestión de incidencias de seguridad	19
Planificación de iniciativas de ciberseguridad industrial	20
03.	
ASPECTOS TÉCNICOS DE LA CIBERSEGURIDAD INDUSTRIAL	21
Conexiones de redes	23
Accesos remotos	23
Uso de normas y patrones	25
Medidas de ciberseguridad industrial	25
04.	
MERCADO DE LA CIBERSEGURIDAD INDUSTRIAL	27
Previsión de nuevas actividades de ciberseguridad industrial	29
Requisitos para nuevos proyectos	30
Contratación de proyectos de ciberseguridad industrial	31
Certificaciones profesionales	32
05.	
CONCLUSIONES	34
06.	
GLOSARIO	35

00.

Introducción

00,
I

DESCRIPCIÓN DEL ESTUDIO
SECTORES ANALIZADOS
AGRADECIMIENTOS

DESCRIPCIÓN DEL ESTUDIO

El estudio se ha realizado de manera conjunta entre el Centro de Ciberseguridad Industrial (CCI) y el Centro Vasco de Ciberseguridad (BCSC, por sus siglas en inglés).

Para llevarlo a cabo se ha encuestado a profesionales de empresas industriales vascas sobre los siguientes dominios de ciberseguridad:

Dominio	Objetivo	Nº de cuestiones
Organización	Analizar las diferentes estructuras organizativas presentes en la Industria Vasca en relación con la Ciberseguridad Industrial	4
Gestión	Identificar el nivel de evaluación del riesgo, así como la planificación de iniciativas y gestión de incidentes de ciberseguridad industrial	3
Aspectos técnicos	Analizar las medidas de protección en el acceso y uso de las tecnologías de automatización y control en la Industria Vasca.	6
Mercado	Identificar las motivaciones para la ejecución de proyectos y la implantación de soluciones de ciberseguridad en la Industria Vasca	7

El periodo de colaboración ha estado abierto desde febrero a junio de 2018, participando un total de **90 empresas industriales**, y representando así mismo una muestra significativa de cada uno de los sectores encuestados, los cuales se indican en el siguiente apartado.”

Este documento presenta los resultados del estudio realizado y proporciona una interpretación de esta basada en el conocimiento y experiencia de sus redactores, así como de los participantes en el proceso de revisión. Confiamos al criterio del lector la obtención de sus propias conclusiones.

Ningún nombre de cliente, proyecto, información técnica o financiera, será revelado en este estudio, el cual contiene únicamente datos cuantitativos consolidados y, por lo tanto, no representa ninguna amenaza para la confidencialidad de las organizaciones participantes.

SECTORES ANALIZADOS

Los encuestados en el estudio son los representantes de organizaciones pertenecientes a sectores con más auge en la región y mayor peso en la economía vasca. Por ello, la mayor parte lo ocupa la fabricación, ingeniería y sector eléctrico, seguidas de “otros” sectores -sin especificar-. También han tenido una participación destacada el sector de las tecnologías de la información y el multisector industrial. Completan la participación, entre otros, sectores de la industria química, transporte, construcción, gas y petróleo, e investigación.

AGRADECIMIENTOS

El Centro de Ciberseguridad Industrial, CCI y el Basque Cybersecurity Centre (BCSC), desean expresar una mención especial, y agradecimiento a las entidades que han colaborado en la difusión del cuestionario de la encuesta:

La Asociación Vasca de Profesionales de Seguridad – Seguritasun Adituen Euskal Elkartea (SAE)

• 9 clústers industriales

- Energía - <http://www.clusterenergia.com>
- FEAF - <http://www.feaf.es>
- MAFEX - <https://www.mafex.es>
- MLC-ITS - <http://www.mlcluster.com>
- PAPEL - <http://www.clusterpapel.com>
- SIDEREX - <https://www.siderex.es>
- SIFE - <http://www.forjas.org>
- UNIPORT - <http://www.uniportbilbao.es>
- ERAIKUNE - <http://www.eraikune.com/>

• 2 clústers no industriales

- GAIA - <http://www.gaia.es>
- EIKEN - <https://eikencluster.com>

Sector de la organización a la que representa

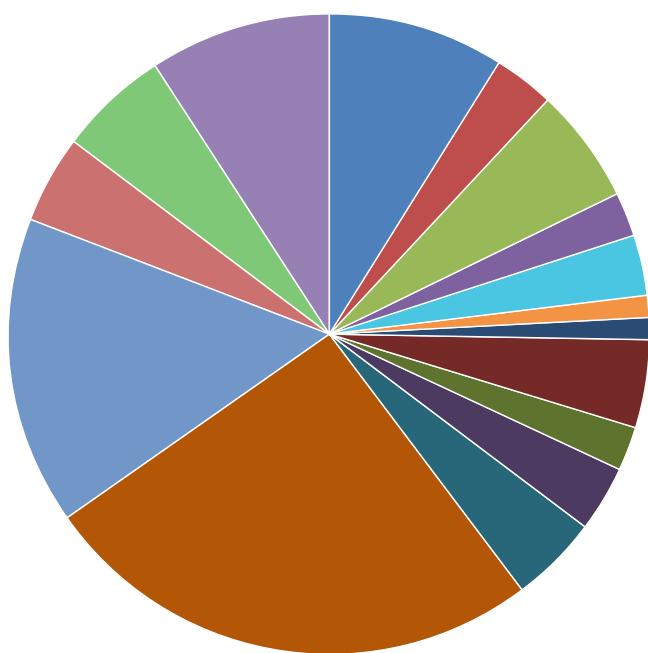


Gráfico - 1. Sectores representados en el estudio.

El estudio cuenta con el respaldo de una gran heterogeneidad de sectores, cuyas empresas pertenecen a un ecosistema global con presencia geográfica tanto nacional como internacional.

Teniendo en cuenta esta diversidad, los datos obtenidos ofrecen un punto de vista amplio y muy descriptivo de los avances que se han producido en Ciberseguridad Industrial en estos últimos años. No sólo en un determinado sector, que pueda gozar de mayor o menor preocupación en lo que a protección de sus redes se refiere, sino a todo el espectro del tejido industrial vasco.

Número de empleados

● De 1 a 9 ● De 10 a 40 ● De 50 a 240 ● De 250 a 499 ● Más de 500



Gráfico - 2. Número de empleados.

Alcance Geográfico

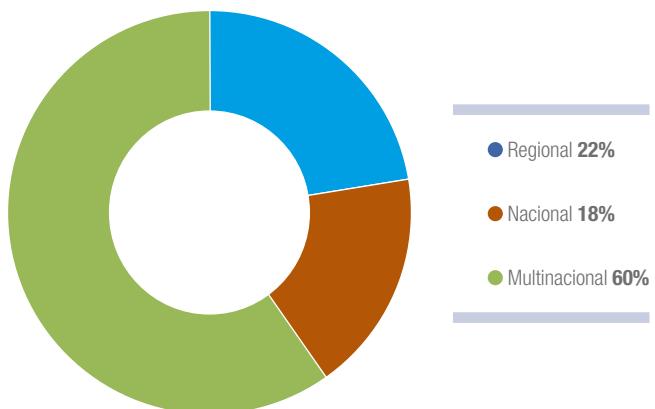


Gráfico - 3. Alcance geográfico.

Facturación Global

● < 2 Millones € ● < 10 Millones € ● < 50 Millones €
● < 200 Millones € ● > 200 Millones €

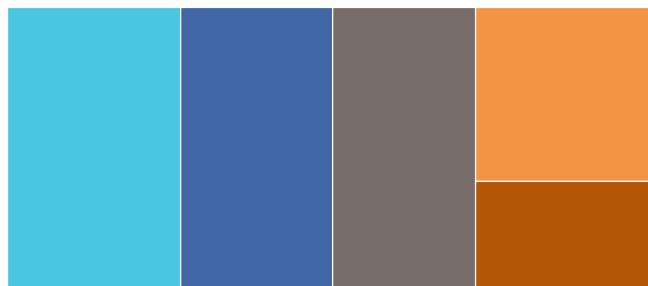


Gráfico - 4. Facturación global.



En base a los datos obtenidos acerca del número de empleados y facturación global, se deduce que una parte significativa de las empresas analizadas corresponden a grandes industrias vascas. Este hecho queda corroborado al observar que el 60% de ellas tienen presencia internacional.

Este tipo de empresas (grandes en contraposición a PYMES) son generalmente las más activas a nivel de protección de sus infraestructuras bien por propia voluntad, por un mayor nivel de concienciación al ser conscientes de su grado de exposición; por recursos o por cumplimiento normativo interno fruto de desarrollo de planes a nivel de consorcio.

Por otra parte, entre las empresas encuestadas, se encuentran infraestructuras críticas de la región. Este hecho, junto con el dato anterior de las grandes industrias vascas analizadas, permiten dotar al informe de especial significancia.

01 .

Organización de la Ciberseguridad Industrial

01



RESPONSABILIDAD RESPECTO A LA CIBERSEGURIDAD INDUSTRIAL GRADO DE CAPACITACIÓN EN CIBERSEGURIDAD INDUSTRIAL

En esta sección debe considerarse que la estructura organizativa de las empresas analizadas es diferente, lo cual puede determinar variaciones en las atribuciones de responsabilidades, implicaciones y capacidades frente a la Ciberseguridad Industrial.

RESPONSABILIDAD RESPECTO A LA CIBERSEGURIDAD INDUSTRIAL

¿Quién(-es) tiene(-n) en su organización la responsabilidad de proteger, en materia de Ciberseguridad, los sistemas de automatización y control industrial?

Los datos confirman la uniforme tendencia en aquellos que han definido la responsabilidad en materia de ciberseguridad, a disgregar dicha responsabilidad entre varias unidades organizativas. Muy pocas de las entidades encuestadas concentran dicho compromiso en un único departamento. Sin embargo, el dato más preocupante es que todavía existe un número de organizaciones que aún no se han enfrentado a la realidad actual, y no han definido tal responsabilidad. En estos casos, la ciberseguridad no es una competencia asignada a ningún área concreta, lo que supone que no se la está dotando a la organización de los recursos y medios necesarios para permitir que se llevan a cabo las medidas.

Responsables de Ciberseguridad

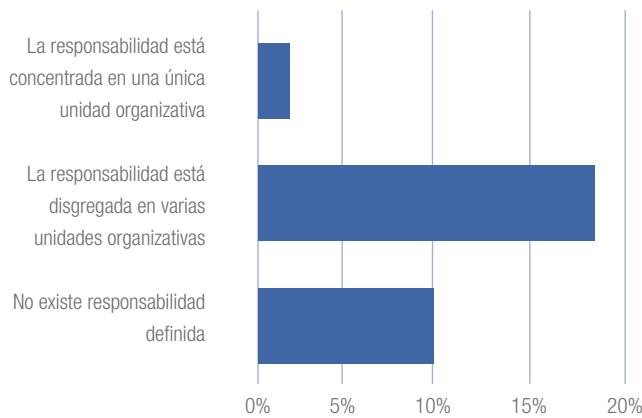


Gráfico - 5. Responsables de Ciberseguridad.

En lo que a unidades departamentales se refiere, buena parte de las entidades encuestadas (70%) asigna dicha tarea al área de tecnologías de la información, enfocando estas acciones desde un punto de vista más lógico que físico o asociado a procesos. Esto puede ser debido a la mayor concienciación y madurez de éstas en materia de ciberseguridad y desde donde se heredan las medidas para hacer frente a los nuevos escenarios.

El resto de las áreas oscilan entre un 10 y un 20%. El área de Automatización de Procesos apenas alcanza el 10%, dato que demuestra posiblemente la falta de conciencia de los de instrumentación y control respecto a los temas de ciberseguridad en su entorno.

Unidades organizativas responsables

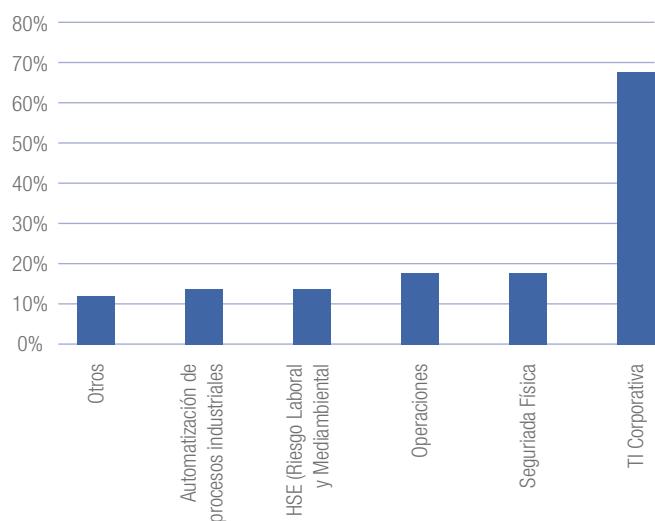


Gráfico - 6. Unidades organizacionales responsables.

¿Cómo participan las distintas áreas de la organización en los aspectos de ciberseguridad?

En relación con el grado de responsabilidad en la protección de los sistemas de control, se observa como el área TI tiene, con diferencia, la mayor implicación. Le siguen las de TO (Tecnologías de Operación), e ingeniería, cuya participación e implicación, aunque menor, también cabe destacar.

¿Cómo participan las distintas áreas de la organización en los aspectos de ciberseguridad?

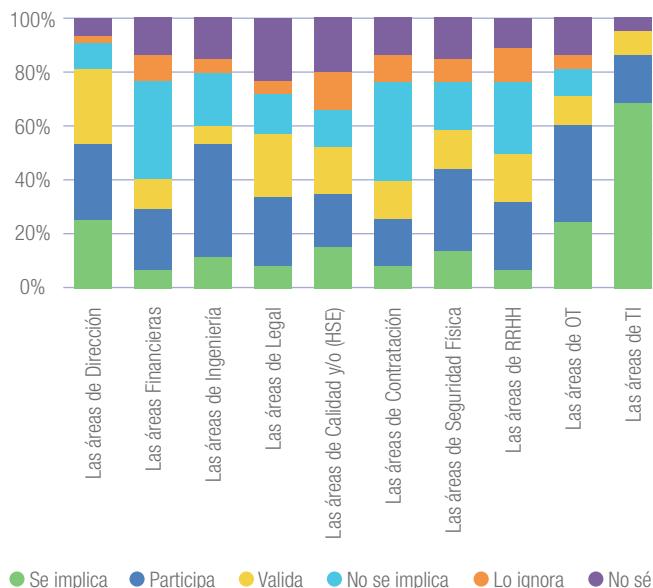


Gráfico - 7. Participación de las áreas de la organización.

¿Los responsables del negocio están sensibilizados con las normas y los riesgos de la Seguridad de las redes industriales?

Los datos muestran que casi la mitad de los responsables del negocio de las empresas estudiadas (48%) se encuentran sensibilizados en un nivel considerado ‘normal’, frente a las normas y riesgos en redes industriales -se entiende por normal el conocimiento de los principales riesgos, amenazas e impactos que tiene para una organización un incidente intencionado, o no, independientemente del sector al que pertenezca-

Por desgracia, todavía el 18% afirma que están muy poco sensibilizado frente a estos riesgos. Sin el respaldo adecuado de la dirección, las iniciativas en esta materia no contarán, probablemente, con apoyo en la toma de decisiones y presupuesto suficiente para poder minimizar y evitar riesgos que afecten a la disponibilidad de las instalaciones. En este contexto, es imprescindible realizar un esfuerzo mayor a nivel directivo, que ayude a tomar conciencia del peligro al que está expuesta la continuidad de negocio dentro de la organización.

Desde el Centro de Ciberseguridad Industrial y el Centro Vasco de Ciberseguridad se trabaja para ayudar a este propósito tanto a directivos como responsables de negocio de organizaciones industriales, de la importancia que tiene hoy en día la tecnología para la sostenibilidad de este, y cómo su pérdida de integridad o disponibilidad puede tener graves consecuencias en la calidad o en la seguridad de los procesos. El documento¹ “*Beneficios de la ciberseguridad para las empresas industriales*”, publicado en 2017, es sólo una muestra del compromiso del CCI en pro del impulso y contribución a la mejora de la Ciberseguridad Industrial.

Por otra parte, desde el Basque Cybersecurity Centre se organizan constantemente jornadas de concienciación enfocadas a los distintos públicos objetivos dentro de los entornos industriales. El objetivo principal de estas jornadas es concienciar acerca de los riesgos más habituales en el ámbito de la ciberseguridad a los que se enfrentan las empresas del mundo OT y fomentar que estas apliquen medidas de ciberseguridad para que estén más protegidas y, por tanto, menos expuestas a las amenazas existentes. De igual modo, la aplicación de este tipo de tecnologías permitirá tener un valor añadido de cara a mantener la capacidad competitiva de dichas empresas.

Esta actividad se alinea con otro tipo de iniciativas públicas que se están llevando a cabo desde el Gobierno Vasco y que buscan respaldar los esfuerzos del sector privado por incrementar su ciberseguridad a través de la formación, subvenciones y otro tipo de ayudas, y, en definitiva, con el objetivo final de situar a Euskadi como un referente en cuanto a la aplicación de ciberseguridad.

Finalmente, en contraposición a lo anterior, un positivo número de ellos (32%) considera el nivel de sensibilización bastante significativo.

¹ Perspectiva sobre el papel habilitador de la ciberseguridad industrial <https://www.cci-es.org/informes-y-analisis-estategicos>

¿Están los responsables del negocio sensibilizados con las regulaciones o los riesgos de ciberseguridad?

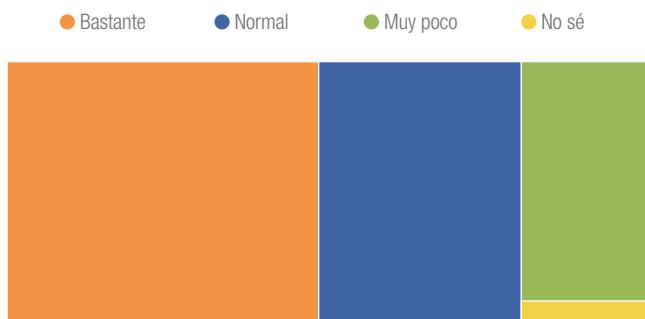


Gráfico - 8. Nivel de sensibilización de los responsables del negocio.

Estas cifras podrían verse mejoradas aumentando, en las distintas jerarquías de la empresa, las actividades de concienciación, tanto a nivel de dirección, como en todas aquellas áreas que puedan tener una mínima relación con la adquisición, validación, gestión y control de las redes y sistemas de la organización.

Es importante señalar que iniciativas regionales impulsadas desde el Gobierno Vasco, y entidades regionales como las del Basque Cybersecurity Centre (BCSC)² han comenzado a permear en la diversa esfera empresarial vasca y se espera que entren con fuerza en todos los niveles organizacionales, especialmente en las empresas públicas e infraestructuras críticas. Esta acción de sensibilización y formación mínima en los conceptos de riesgo y medidas de protección general debe ser diseñada específicamente para cada sector. De esta manera cada uno de ellos, podrá ver claramente las ventajas de su implementación respecto a sus competencias y responsabilidades sobre los activos de la empresa.

El objetivo hacia el que deben orientarse estos programas de debería estar centrado en los beneficios que tiene la ciberseguridad sobre la calidad, resiliencia y la seguridad de los procesos y, por lo tanto, lograr el compromiso con la ciberseguridad de una manera holística dentro de todos los niveles de la organización.

GRADO DE CAPACITACIÓN EN CIBERSEGURIDAD INDUSTRIAL

¿Cuál es el grado de capacitación de su organización en Ciberseguridad Industrial?

En clara concordancia con los niveles de participación por departamentos en los aspectos de la ciberseguridad, nos encontramos el siguiente gráfico, que relaciona el nivel de capacitación en esta disciplina, con las unidades organizacionales. La capacitación de las empresas en materia de Ciberseguridad Industrial, obviamente, varía según los distintos departamentos. Aunque el motor económico de la empresa sea su área de producción -donde las tecnologías de automatización y control son vitales-, las empresas industriales vascas muestran mayor capacitación en los departamentos que están directamente relacionados con la Seguridad de la información (T.I.) que en los responsables del mantenimiento de los procesos de negocio (T.O.).

¿Cuál es el grado de capacitación de su organización en Ciberseguridad Industrial?

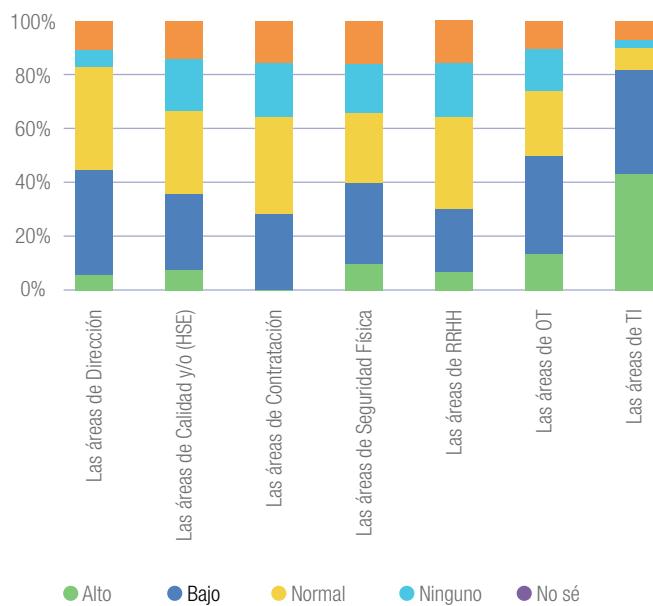


Gráfico - 9. Comparativa del nivel de capacitación de los equipos de trabajo.

² <https://www.basquecybersecurity.eus/es/>



Es por tanto una tarea fundamental de los responsables vinculados con el negocio, lograr un alto grado de resiliencia, que requiere capacitación específica frente la protección frente a las amenazas o errores humanos, que puedan entorpecer el correcto funcionamiento de los procesos de producción.

Un dato bastante notable es que gran número de los encuestados considera que los empleados en las áreas de OT poseen un nivel bajo (28%) o normal (38%) de capacitación, y solo un 12% de los gestores considera que su equipo de automatización esté adecuadamente formado. Incluso, un 14% considera que hay una falta total de capacitación en dicho equipo. Se hace imprescindible, por tanto, que las empresas inviertan en formación del personal relacionado con los aspectos de Tecnologías de la Operación y su seguridad tecnológica.

02.
I

Gestión de la Ciberseguridad Industrial

02.



EVALUACIÓN DE RIESGOS
GESTIÓN DE INCIDENCIAS DE SEGURIDAD
PLANIFICACIÓN DE INICIATIVAS DE CIBERSEGURIDAD INDUSTRIAL

EVALUACIÓN DE RIESGOS

¿Su empresa ha realizado evaluaciones del nivel de riesgo de los sistemas de automatización y control?

En lo que respecta a la realización de evaluación de riesgos en redes industriales, las cifras son alarmantes y muestran una baja preocupación por analizar la situación real de exposición que tiene la tecnología que opera el proceso industrial de la organización. En concreto, un 42% reconoce no haber realizado ninguna evaluación del nivel de riesgo de sus sistemas de automatización y control. Por tanto, aparte de no saber las consecuencias a las que se enfrentan, tampoco disponen de información acerca del estado de madurez en el que se encuentran, por lo que difícilmente podrán hacer una gestión y priorización eficiente de los recursos necesarios cara a ejecutar un proyecto de estas características.

Entre el conjunto de las evaluaciones realizadas, destaca con un 38% la referente a la capacidad organizativa, que incluye, entre otras variables, las políticas y procedimientos establecidos. Casi 38% de los encuestados declara haber llevado a cabo otros dos tipos de evaluaciones: técnicas sobre las redes; como análisis de vulnerabilidad, de segmentación y test de intrusión; y normativas, cumplimiento de distintas normas y estándares como NERC-CIP, IEC 62443, el Sistema de Gestión de la Ciberseguridad Industrial - SGCI de CCI³, entre otras.

¿Se ha evaluado en su organización el nivel de riesgo de los sistemas de control y automatización?

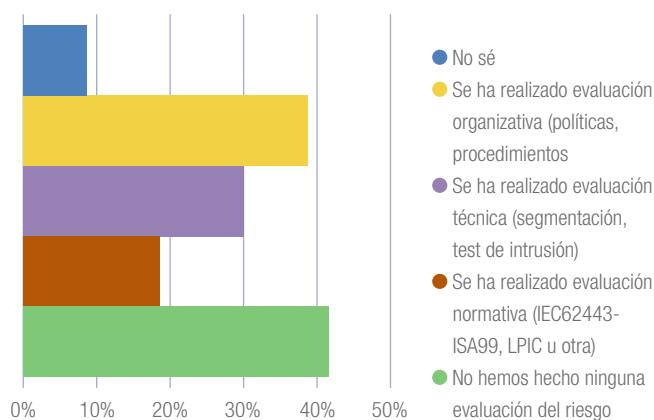


Gráfico - 10. Análisis de riesgos en sistemas de control y automatización industriales.

³ <https://www.cci-es.org/sgci>

GESTIÓN DE INCIDENCIAS DE SEGURIDAD

¿Cómo es el proceso de Gestión de Incidencias de Seguridad en las redes de automatización de su empresa?

Solo el 12% de las empresas analizadas afirma tener un proceso desarrollado y en aplicación de Gestión de Incidencias de Ciberseguridad Industrial. En el 27% de las empresas este proceso no existe, y otro 27% actúa de forma reactiva. Por otro lado, el 23% de las empresas afirma estar definiendo este proceso, el cual es necesario como se evidenció en los eventos con impacto global ocurridos en el 2017. Nos referimos indudablemente a muestras de malware como WannaCry, Petya, Crashoverride, afectando sectores como el automovilístico, marítimo, distribución energética o petroquímico. Pero no sólo hemos de fijarnos en el hecho en sí, sino la evolución que están experimentando. Tal es el caso de los sistemas de seguridad funcional safety de plantas industriales que han comenzado a verse afectado a través del malware Titón/Trisis/Hatman así como, es cada vez más frecuente, el uso de los dispositivos IoT para ataques de denegación de servicio masivo, entre otros.

¿Cómo es el proceso de gestión de incidentes de ciberseguridad en el ámbito industrial de su organización?

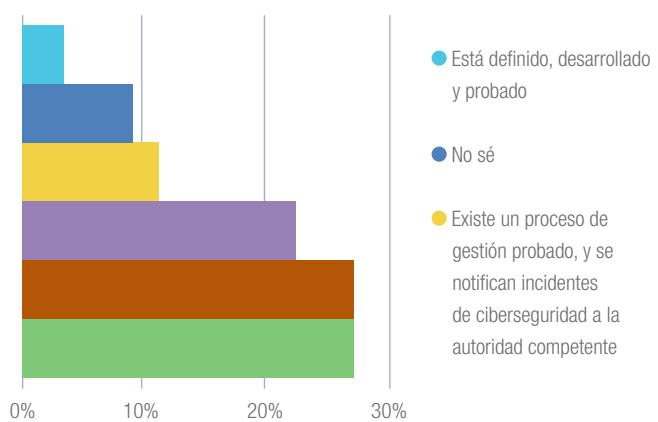


Gráfico - 11. Gestión de Incidencias de Seguridad Industrial.

Por esto, los últimos años han sido decisivos para las organizaciones en materia de ciberseguridad, poniendo a prueba

sus procesos de gestión de incidentes. Los acontecimientos mundiales en los que miles de dispositivos se han visto involucrados han demostrado que los procedimientos de actuación deben estar perfectamente planificados y con la implicación adecuada de todos los afectados -desde la dirección al último eslabón de la cadena-, para ser efectivos.

Debe existir una coordinación con los organismos externos adecuados -CERT y/o CSIRT-. Como es el caso del Basque Cybersecurity Centre (BCSC) el cual proporciona apoyo y consejo a los usuarios que se ven afectados por un incidente de ciberseguridad guiándoles sobre las pautas a seguir y, en el caso de que sea necesario, se le redirige al punto de contacto más adecuado según corresponda. Así mismo, se trabaja de manera conjunta y coordinada con multitud de organizaciones y equipos de respuesta a incidentes tanto a nivel nacional como internacional, de ámbito público y privado, de cara a dar una respuesta conjunta y coordinada a las ciberamenazas.

Las distintas iniciativas de intercambio de experiencias, tanto positivas como negativas, en los distintos aspectos de la ciberseguridad industrial, permite a la comunidad obtener valiosa información que mejora los distintos procesos relacionados con la ciberseguridad, y más en concreto, para el caso de la gestión de incidentes.

PLANIFICACIÓN DE INICIATIVAS DE CIBERSEGURIDAD INDUSTRIAL

¿Cómo se planifican habitualmente en su empresa las iniciativas de Ciberseguridad Industrial?

En relación con la planificación de las iniciativas de Ciberseguridad Industrial, es significativo observar una fuerte disparidad de actuaciones. Mientras que el 21% de las empresas reconocen seguir recomendaciones de una consultora externa, otro 21% afirma seguir recomendaciones de la operativa interna. Un 18% planifican, diseñan y ejecutan las iniciativas a lo largo del tiempo, y un 12% reconoce promover iniciativas bajo la adecuación de directrices mínimas marcadas por legislación. Revelador es también el número de aquellas que solo actúan bajo reacción ante algún incidente (17%).

Es importante advertir que limitarse a mantener el grado de inversión en ciberseguridad en el mínimo que permite el cum-

plimiento legislativo implica que nuestros niveles de protección estarán muy por debajo del estándar necesario para hacer frente a los peligros y riesgos actuales a corto plazo. Las leyes y normativas de los Estados son siempre lentas, lo cual es especialmente visible en términos técnicos complejos y alejados de los legisladores, como la Ciberseguridad industrial. Tanto la tecnología como la ciberdelincuencia evoluciona a gran velocidad, y más en concreto en el segundo de los términos, con mayor grado de sofisticación y mejora.

¿Cómo se planifican habitualmente las acciones de Ciberseguridad Industrial en su organización?

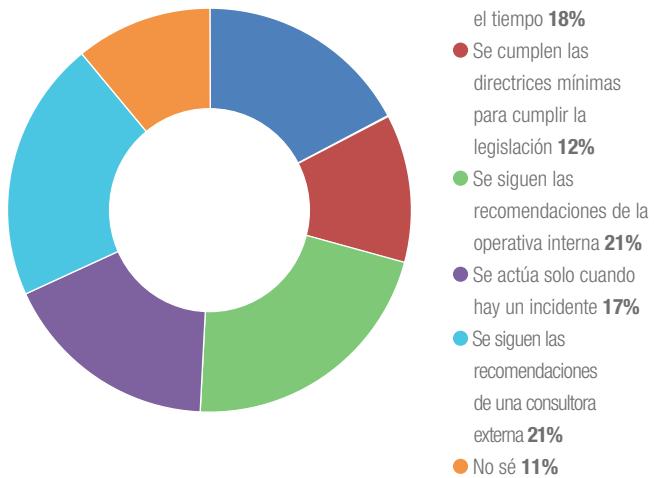


Gráfico - 12. Planificación de iniciativas de Ciberseguridad Industrial.

03.

Aspectos técnicos de la Ciberseguridad Industrial



03.

CONEXIONES DE REDES

ACCESOS REMOTOS

USO DE NORMAS Y PATRONES

MEDIDAS DE CIBERSEGURIDAD INDUSTRIAL

CONEXIONES DE REDES

¿Las redes de automatización de su empresa están segmentadas y protegidas?

En los últimos años, las organizaciones industriales han visto cómo sus dispositivos han evolucionado obligando a modificar muchas de las estructuras adoptadas para proteger a la propia organización. Las arquitecturas de red que tantos años habían soportado un tráfico aislado, constante y seguro, son modificadas para adecuarse a las nuevas demandas como el mantenimiento predictivo, logística adaptativa, mejora de procesos, trazabilidad inteligente, entre otras. Se requiere de una integración de TI y TO, que puede poner en riesgo la continuidad del negocio si no se despliegan las medidas oportunas.

Más de la cuarta parte (22%) de las empresas industriales estudiadas afirman que existe una separación total entre sus redes, principalmente, la corporativa e industrial.

¿Están segmentadas y protegidas las redes en la organización?

- La red corporativa e industrial están conectadas directamente
- No sé
- La red industrial está total y físicamente aislada de la red corporativa/ofimática
- La red industrial tiene distintos niveles de segmentación
- La red corporativa e industrial están segmentadas por un dispositivo de filtrado

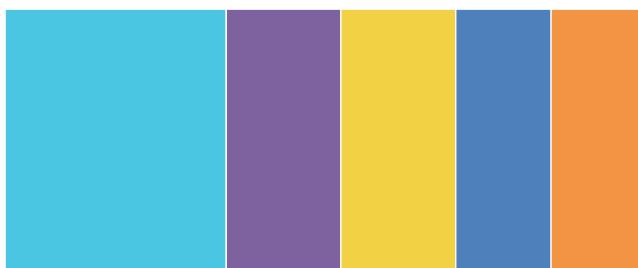


Gráfico - 13 Segmentación y protección de redes de automatización.

El porcentaje más significativo de las empresas que reconocen tener establecida conexión entre la red corporativa y las redes industriales están segmentadas por un cortafuegos (40%) o con distintos niveles de segmentación mediante varios dispositivos de filtrado (22%). Sin embargo, existe un muy preocupante 17% de empresas que mantiene sus redes directamente conectadas, lo que representa un enorme riesgo de

incidencias de seguridad. Obviamente, este último grupo de empresas debe encontrarse entre aquellas que reconocían no haber realizado evaluación de riesgos, por lo que no cuentan con una percepción real del peligro que supone mantenerlas conectadas sin ningún tipo de filtro para controlar el acceso y su tráfico.

ACCESOS REMOTOS

¿Su red industrial posee dispositivos conectados a Internet, independientemente de los mecanismos de protección aplicados?

La mayoría de las empresas estudiadas (45%) afirma tener dispositivos que están conectados a Internet de forma permanente. Desciende al 30% aquellos cuya conexión a internet es solo activada bajo demanda, y un 12%, el de los que manifiestan no tener ningún tipo de dispositivo en red abierta. En caso de ser necesario el acceso desde infraestructuras externas a la red de control, la utilización de soluciones VPN aporta el cifrado y autenticación necesarios para proteger estas conexiones. El uso de un software y/o hardware especializado para acceso remoto, así como una adecuada política de seguridad relativa al mantenimiento de actualizaciones, de gestión de acceso y usuarios es imprescindible para reducir el riesgo que puede suponer un acceso indebido a los sistemas de operación.

¿Tiene su red industrial, o alguno de los dispositivos o sistemas albergados en ella, conexión a internet (independientemente de los mecanismos de protección aplicados)?

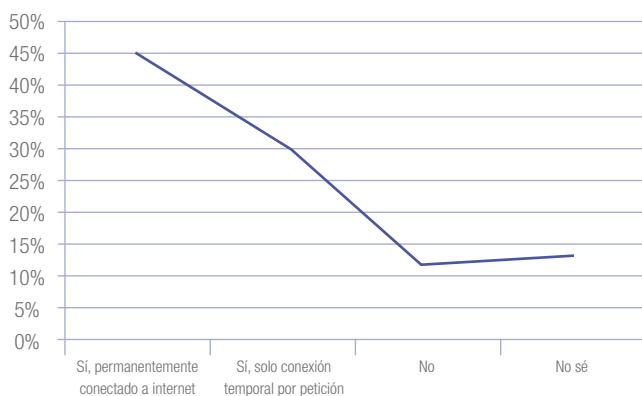


Gráfico - 14. Dispositivos de redes de automatización conectados a Internet.

Es preocupante el alto porcentaje de aquellos que manifiestan desconocer si disponen de dispositivos conectados a internet (13%), especialmente si se trata de conexiones permanentes. En este caso, implica falta de protección, y por lo tanto la exposición de dispositivos que pueden poner en riesgo la disponibilidad o integridad de los sistemas que operan los procesos críticos.

Actualmente existen distintas iniciativas que facilitan la detección de IPs expuestas -p.e. la bien conocida Shodan, Censys o ZoomEye⁴-, herramientas que permiten el filtrado por diversos campos, de forma que el usuario, sin necesidad de grandes conocimientos en la materia, es capaz de detectar equipos expuestos y vulnerables dentro de su organización. Por ello, es necesario realizar una evaluación del nivel de exposición de nuestras redes y dispositivos, para controlarlos y gestionarlos de forma correcta.

La existencia de sistemas de control industriales accesibles desde Internet, combinada con la escasa seguridad incorporada y el nivel de criticidad asociada a los procesos controlados por éstos, hace que el riesgo inaceptable e inasumible para las organizaciones industriales.

¿Su red industrial posee accesos remotos?

El alto grado de especialización de los entornos industriales requiere de proveedores capaces de cubrir la demanda tecnológica que las propias organizaciones no son capaces generar para llevar a cabo sus procesos. Es por esto por lo que, una vez desplegadas las instalaciones, sistemas o equipamiento, es necesario un apoyo que haga frente a necesidades futuras, tanto por incidencias o solicitudes. Siempre y cuando sea posible, cabe la posibilidad de realizarlo de forma remota, lo cual abarata los costes generados por desplazamiento de técnicos especialistas.

Muchas son las actuaciones que requieren una supervisión continua -24 horas, 365 días- en dispositivos de alta producción, soporte y mantenimiento por parte de los proveedores IT, OT, etc, etc. En un mundo hiperconectado, la industria 4.0 es ya una industria altamente dependiente de las redes.

¿Se dispone de acceso remoto a la red industrial que permita la supervisión y/o control de sus sistemas?

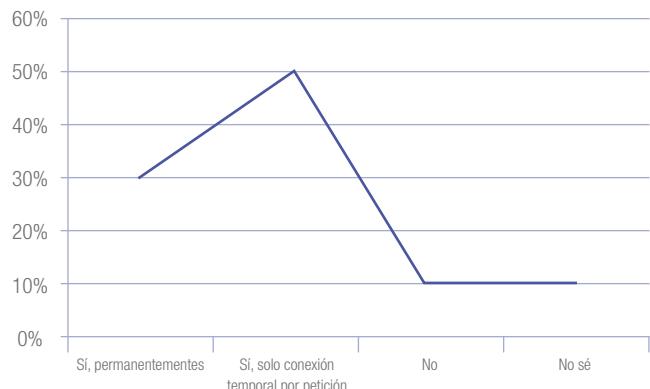


Gráfico - 15. Acceso remoto

En caso afirmativo en la pregunta anterior, ¿por qué motivo?

El principal motivo para el establecimiento de accesos remotos a los sistemas de control industriales de las empresas estudiadas es la gestión de estos; así lo declara un alto porcentaje de los encuestados (77%). De ellos, un 37% accede a la red industrial para realizar labores de soporte y mantenimiento en remoto por terceras partes. Esta situación aumenta el riesgo para las distintas organizaciones. Dichos proveedores requieren de conectividad a las instalaciones para poder llevar a cabo las tareas para las que han sido contratados, por lo que, salvo que existan alternativas a ello, deberemos permitir el acceso a equipos fuera de nuestro control, con desconocimiento pleno de uso, estado y nivel de seguridad. Además, esto se agrava cuando el mismo debe ser local, lo cual genera conectividad en el mismo entorno sin paso por ningún elemento de seguridad perimetral. Esta debería ser razón suficiente para exigir requisitos de ciberseguridad a terceros que prestan servicios en el entorno industrial.

⁴ <https://www.shodan.io/> Shodan es el primer motor de búsqueda del mundo para dispositivos conectados a Internet.
<https://censys.io/>
<https://www.zoomeye.org/>

¿Cuál es el motivo para tener accesos remotos a la red industrial?

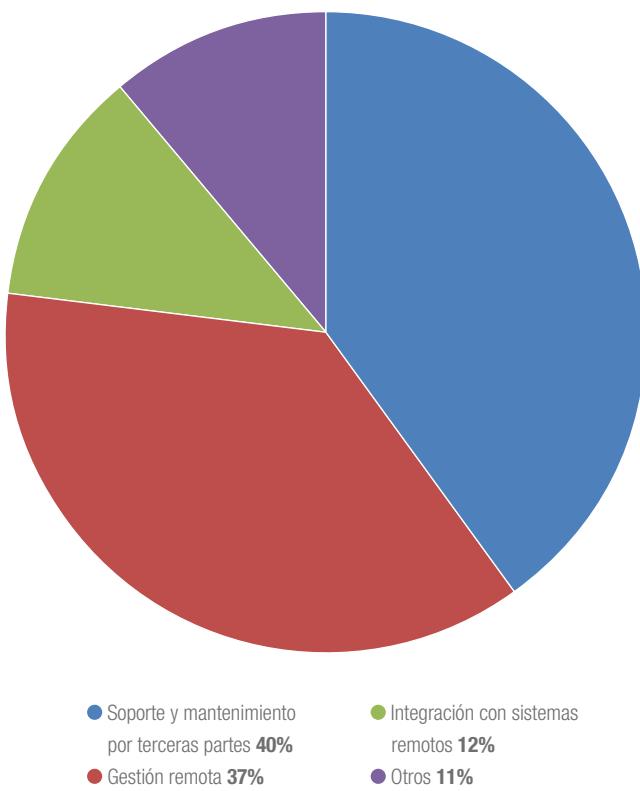


Gráfico - 16. Motivos para la utilización del acceso remoto.

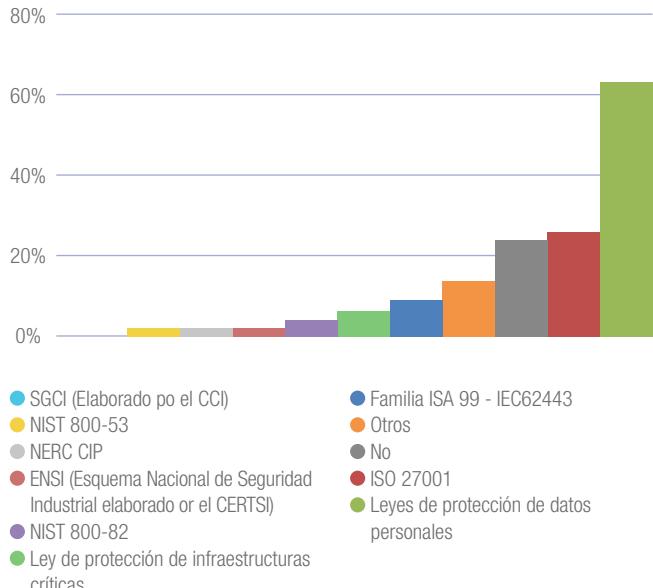
USO DE NORMAS Y PATRONES

¿Qué normas se utilizan en el ámbito de la Ciberseguridad Industrial de su empresa?

La mayor parte de las empresas utilizan normas para el establecimiento de la Ciberseguridad Industrial de la empresa, aunque un número importante reconoce no hacerlo (23%).

Encuentra fuerte cabida en el gráfico la aplicación de las Leyes de Protección de Datos Personales (64%), la familia ISO 27001 (25%), seguidas de la familia IEC 62443 (Antes ISA-99) y la Ley de Protección de las Infraestructuras Críticas. Esto dato, pone de manifiesto que, aunque se estén aplicando normativa en entornos de operación, no se está haciendo de forma correcta ya que, como norma general, los sistemas de operación no deberían almacenar datos de carácter personal o confidencial.

¿Están utilizando normas y estándares en el ámbito industrial?



De entre aquellas específicas para la Ciberseguridad Industrial, aparecen la guía SGCI del CCI, y las reglamentaciones sectoriales, como NERC CIP enfocada a la protección de infraestructuras críticas de sistemas de energía eléctrica. Destacando claramente con más de un 60% la protección de datos personales y más de un 20% ISO 27001 lo que constata que las organizaciones industriales vascas están centrando sus esfuerzos en la protección de los sistemas de información y de forma muy reducida en los sistemas de operación, especialmente en aquellos casos en los que las organizaciones son también operadores de infraestructuras críticas y están obligados por ley.

MEDIDAS DE CIBERSEGURIDAD INDUSTRIAL

¿Qué medidas de Seguridad industrial ya ha implementado su empresa?

Casi todas las empresas analizadas afirman tener implantado algún tipo de medida de Ciberseguridad Industrial. De las medidas técnicas, las más habituales (por orden de mayor a menor influencia) son las soluciones automatizadas de copias de seguridad, antivirus, firewalls convencionales y, entre las

medidas de gestión, destaca el mantenimiento de la arquitectura de red documentada.

También ocupan un lugar importante los firewalls industriales, y la definición de políticas y procedimientos.

IT disminuyan en beneficio de las diseñadas específicamente para entornos OT. Esto requiere de una adaptación de las soluciones IT a las necesidades y particularidades industriales. Tal es el caso, de los cortafuegos, los cuales paulatinamente, irán ocupando mayor presencia en este gráfico hasta que, aquellos diseñados para entornos IT, llegan a perder protagonismo.

¿Qué medidas tiene implantadas la organización en el ámbito industrial?

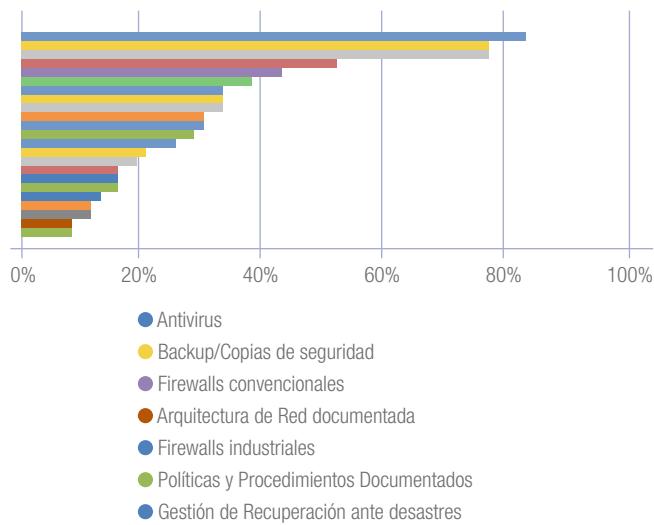


Gráfico - 18. Medidas de Seguridad Cibernetica Industrial utilizadas.

Existen diversas medidas de ciberseguridad implantadas en las redes y sistemas industriales actualmente, sin embargo, no todas ellas son igual de eficaces. Algunas, son aplicadas en estos entornos sin el criterio adecuado, esto es, provienen de entornos IT sin capacidades para entornos OT. Por ejemplo, el tráfico que soportan los entornos industriales tiene unas características concretas, particularmente en lo que a protocolos se refiere, específicos muchos de ellos al campo de aplicación. la creación de ciertos patrones de comportamiento limitados para cada dispositivo de filtrado de tráfico (respecto a dispositivos que pueden comunicarse, intercambiando información limitada, y con permisos predefinidos, entre otras variables). De esta forma, se adaptan las herramientas, y se convierten en más potentes y eficientes para desarrollar su trabajo en entornos OT.

Poco a poco, la mayor concienciación e información de los responsables de ciberseguridad industrial, contribuye a que las cifras de implantación de dispositivos provenientes del mundo

04.

Mercado de la Ciberseguridad Industrial



04.

PREVISIÓN DE NUEVAS ACTIVIDADES DE CIBERSEGURIDAD INDUSTRIAL
REQUISITOS PARA NUEVOS PROYECTOS
CONTRATACIÓN DE PROYECTOS DE CIBERSEGURIDAD INDUSTRIAL
CERTIFICACIONES PROFESIONALES

PREVISIÓN DE NUEVAS ACTIVIDADES DE CIBERSEGURIDAD INDUSTRIAL

¿Tienen previsto iniciar nuevas actividades en el ámbito de la Ciberseguridad Industrial?

Un determinante 80% de las empresas estudiadas prevé iniciar actividades de Ciberseguridad Industrial, y 10% de ellas lo hará en el próximo año. Un 40% se encuentra ya en fase de implementación en los próximos 6 meses, contando por tanto con presupuesto específico asignado. Solamente el 20% de las empresas estudiadas todavía no contempla las acciones de Ciberseguridad Industrial en sus presupuestos.

¿Tiene previsto iniciar nuevas actividades en el ámbito de la Ciberseguridad Industrial?



Gráfico - 19. Previsión de nuevas actividades en Ciberseguridad Industrial.

Las conclusiones más inmediatas que se desprenden de la inminente demanda, es la necesidad de una oferta más amplia, tanto en el sentido de número de proveedores, como en la diversidad de productos y servicios adaptados a las necesidades de cada sector, y cliente. En este sentido, desde 2016, el Centro de Ciberseguridad Industrial viene publicando un catálogo⁵ de proveedores de servicios y soluciones de ciberseguridad industrial, el cual caracteriza la industria de proveedores en este campo. Por otro lado, se hace imprescindible que todas las acciones que se lleven a cabo en el ámbito de la ciberseguridad industrial dentro de las organizaciones estén lideradas, controladas, gestionadas y supervisadas por la figura interna

del 'Responsable de Ciberseguridad Industrial'. Sigue siendo elevado el número de organizaciones que no han designado dicho responsable, por lo que estas acciones, en última instancia, no cuentan con la implicación y respaldo de una persona capacitada -en formación, presupuesto, y autoridad de decisión dentro de la organización.

En lo referente a formación, es también esta una gran oportunidad para muchos profesionales al crearse una fuerte demanda para ellos. Los profesionales tienen la posibilidad de diversificar o reconvertir sus carreras profesionales, y para ello necesitarán entrenamiento y formación, lo que contribuirá también al desarrollo del mercado educativo específico. Con el doble objetivo de proporcionar una formación profesional de calidad con un enfoque práctico y la flexibilidad que necesitan los profesionales y sus organizaciones. CCI ha puesto en marcha en este 2018 la Escuela Profesional de Ciberseguridad Industrial⁶, la cual se suma a otras iniciativas puestas en marcha como el Máster de Ciberseguridad de la Universidad de Mondragón; las jornadas divulgativas del Colegio Oficial de Ingenieros Industriales de Álava, y encuentros como Indussec 2018, IndustrySec 2018, el Basque Cybersecurity Day o la BIMH.

¿Cuáles son las motivaciones para la ejecución de proyectos y la implantación de soluciones de Ciberseguridad Industrial?

¿Cuales son las motivaciones para la ejecución de proyectos e implantación de soluciones de ciberseguridad en el ámbito industrial?

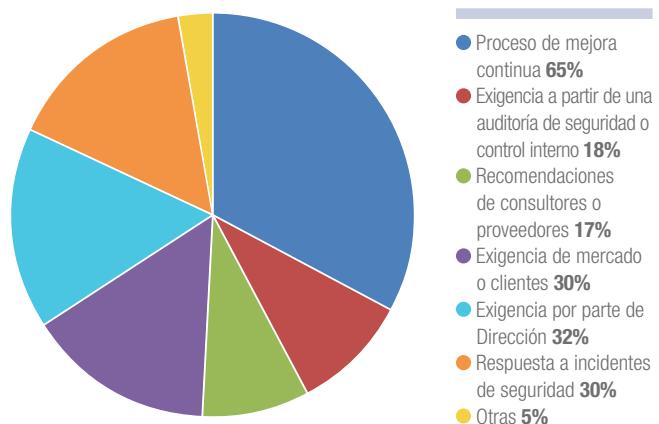


Gráfico - 20. Motivación para la ejecución de Proyectos de Ciberseguridad Industrial.

⁵ <https://www.cci-es.org/catalogo>

⁶ <https://www.cci-es.org/escuela> Escuela Profesional de Ciberseguridad Industrial del Centro de Ciberseguridad Industrial

Las empresas encuestadas muestran cierta disparidad en lo que respecta a las motivaciones a la hora de aplicar medidas de ciberseguridad industrial. La principal motivación, la mejora continua con un 65%. Es coherente con el escenario actual, en el que las amenazas a los procesos industriales están cambiando debido a la introducción de componentes tecnológicos como la integración con tecnología de la información, que incorporan un beneficio, también un riesgo para el cuál las industrias no están preparadas.

Asociado a esta misma razón, el 30% reconoce aplicar medidas como respuesta a incidentes de ciberseguridad, de nuevo como método imprescindible para adaptarse al nuevo entorno. Es significativa la amplia presencia de otros factores importantes en este contexto, como las exigencias por parte de la Dirección, y las necesidades del mercado. Esto revela un incremento de la madurez en la gestión de este riesgo, que exige al mercado y a las empresas reconocer la demanda y necesidad de implantar soluciones específicas de Ciberseguridad Industrial.

En su opinión, ¿cuál es la tendencia de las inversiones financieras de su empresa en Ciberseguridad Industrial para los próximos años?

Buena parte de las empresas estudiadas (85%) consideran que la inversión en Ciberseguridad Industrial se incrementará, mientras que unánimemente un 15% considera que se mantendrá y nadie ha considerado que disminuirá.

En su opinión ¿Cuál será la evolución de cara al futuro en inversión de recursos humanos y presupuesto en Ciberseguridad Industrial, incluyendo su aplicación a Industria 4.0?

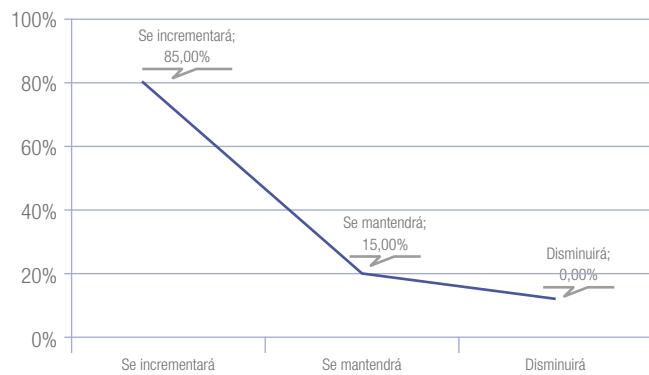


Gráfico - 21. Tendencia de las inversiones en Ciberseguridad Industrial.

REQUISITOS PARA NUEVOS PROYECTOS

¿Se incluyen requisitos de Ciberseguridad Industrial en los nuevos proyectos de la empresa?

La mayoría de las empresas industriales estudiadas contemplan requisitos básicos o completos de Ciberseguridad Industrial en todos los aspectos de sus nuevos proyectos. Sin embargo, todavía es muy preocupante que un 22% de las empresas no lo considere. Sin duda, este escenario irá evolucionando a medida que aumente la concienciación de los equipos de desarrollo e integración de tecnologías de automatización frente a la Ciberseguridad Industrial. Y como no, en aquellos casos en los que un incidente de ciberseguridad haga saltar las alarmas y estimular las decisiones de Dirección, de forma que los presupuestos pasen a incorporar una partida presupuestaria específica para la aplicación de ciberseguridad en todas y cada una de las fases del ciclo de vida de los proyectos de la organización.

¿Se incluyen requisitos de ciberseguridad industrial en los proyectos nuevos o recientes (como por ejemplo, los de adaptación a Industria 4.0)?

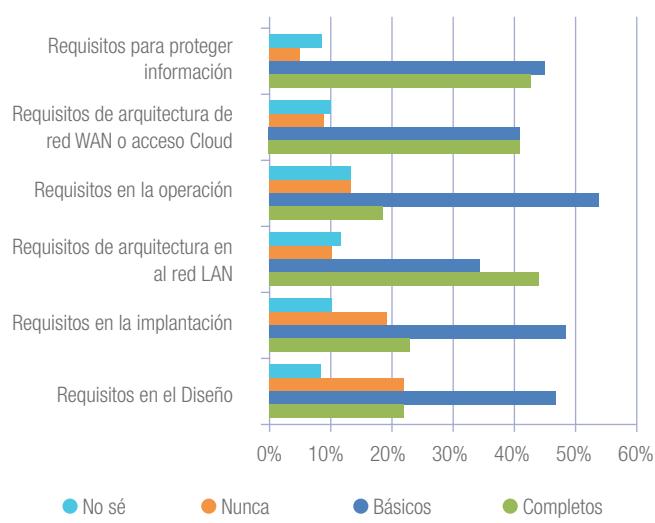


Gráfico - 22. Requisitos de Ciberseguridad Industrial en nuevos Proyectos.

CONTRATACIÓN DE PROYECTOS DE CIBERSEGURIDAD INDUSTRIAL

En su empresa, ¿quién toma la decisión sobre contratación de proyectos de Seguridad Digital para las redes de automatización?

La gran parte de las decisiones sobre contratación de Ciberseguridad Industrial las realiza según el estudio el área de TI (68%) sobre quien previamente hemos visto recae la mayor implicación y participación en las tareas de ciberseguridad industrial. Con un 28%, el área de negocio también participa en la toma de decisiones en este ámbito.

Solo un 7% de las empresas otorgan la decisión de contratación al área de automatización de procesos, probablemente con el mayor desconocimiento aún imperante entre su personal.

Otro 18% supone el número de encuestados que manifiestan que las decisiones de contratación son tomadas por cada una de las unidades organizativas a los que aplica (cada área su parte).

¿Quién toma en la organización las decisiones de contratación de los proyectos de ciberseguridad?

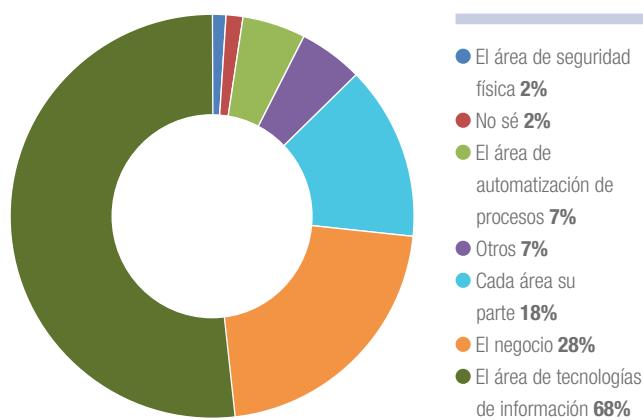


Gráfico - 23. Decisiones de contratación.

¿Cuáles son los proveedores de Ciberseguridad para redes de automatización de su empresa?

En cuanto al tipo de empresas proveedoras de Ciberseguridad para empresas industriales, el estudio muestra que existe una clara inclinación por las empresas consultoras especializadas en ciberseguridad (52%). Sin embargo, también es notorio el número de aquéllas que declaran proporcionar dichos servicios de forma interna (40%), aunque esta decisión pueda traer acarreado la falta de profesionales cualificados.

Algo más lejos en cifras aparecen los fabricantes de ciberseguridad (23%), las ingenierías o integradores industriales con alianzas con especialistas en ciberseguridad industrial (17%), seguidos por los fabricantes industriales con alianzas con especialistas en ciberseguridad (15%).

¿Quienes son los proveedores de ciberseguridad en su organización?

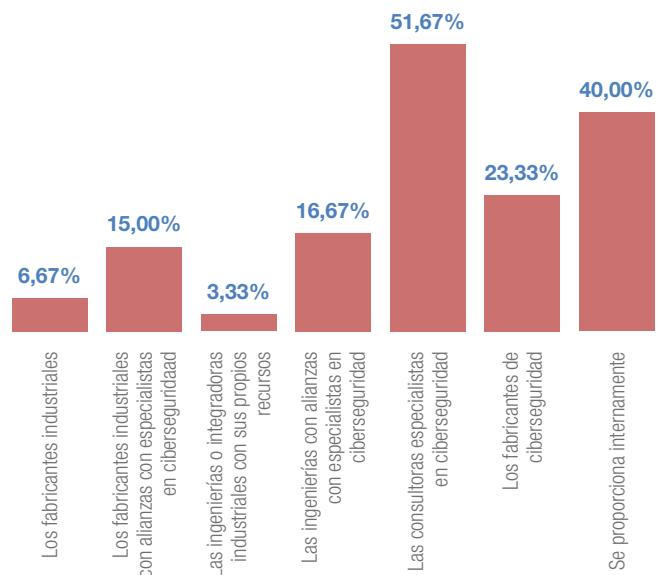


Gráfico - 24. Proveedores de Seguridad Cibernética Industrial.

CERTIFICACIONES PROFESIONALES

¿Cómo valora usted las certificaciones profesionales del equipo de proveedores a la hora de contratar servicios de Ciberseguridad Industrial?

La cualificación del personal responsable de llevar a cabo proyectos o implantar soluciones de ciberseguridad es la variable que influye de forma definitiva a la hora de seleccionar y poner en marcha las medidas más adecuadas a las necesidades y características de cada organización. Las organizaciones encuestadas son conscientes de ello y por ello mayoritariamente han valorado de forma positiva la existencia de certificaciones profesionales entre el personal de los proveedores de servicios de Ciberseguridad Industrial. Los resultados muestran una valoración muy positiva (27%) o positiva (68%), y solo un 5% de las empresas considera baja la utilidad y valor de las referidas certificaciones.

Desde el CCI consideramos las certificaciones profesionales o credenciales un aval, al menos un requisito mínimo, de los conocimientos, experiencia y preocupación por la continua puesta al día de quien las ostenta. Esto las convierte en un criterio de valor que debe tenerse en cuenta en todo proceso de selección de personal y, por ende, de proveedores que presten servicios de Ciberseguridad Industrial. Por este motivo, CCI cuenta con su propio sistema de credenciales⁷, tanto para profesionales como para estudiantes, a través de cual pretende fomentar el compromiso con la calidad profesional, formación, conocimientos y experiencia- de unos, y la vocación temprana en otros. El objetivo de este proyecto es, precisamente, el reconocimiento de aquellos profesionales de su ecosistema ocupados y preocupados por la ciberseguridad industrial y las consecuencias de “lo ciber” en el seno de sus organizaciones, o como eje central de su formación, y que demuestren un compromiso con el desarrollo de esta disciplina.

¿Cómo valora las certificaciones profesionales del equipo del proveedor a la hora de contratar servicios en este ámbito?

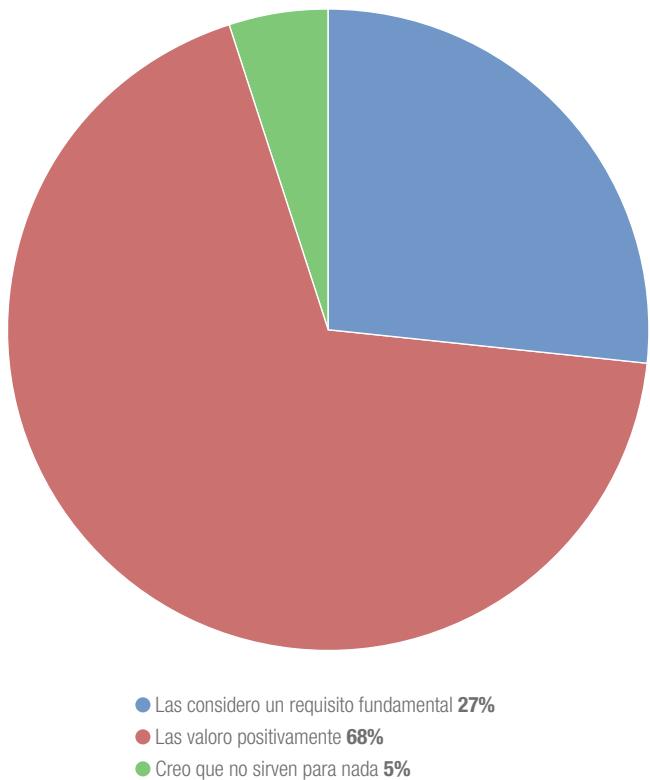


Gráfico - 25. Valoración de la importancia de las certificaciones.

⁷ <https://www.cci-es.org/credenciales>

05.

Conclusiones

- Claramente la gestión del riesgo en los sistemas de automatización y control está siendo asumida por el área de tecnologías de la información, enfocando sus acciones desde un punto de vista más cibernético que físico o asociado a procesos. Esto es debido a la mayor madurez de estas áreas en materia de ciberseguridad, frente a las áreas técnicas de la operativa industrial. Es decir, en la mayoría de los casos se aborda el problema con una visión parcial, muy informática, por lo que sería conveniente darle una visión más global de gestión de riesgos del negocio.
- Es preciso elevar el nivel de concienciación frente a la necesidad y las implicaciones de la Ciberseguridad Industrial a todos los niveles de la organización. De los datos recabados se puede inferir que hay reticencia a la hora de reconocer y notificar los impactos derivados de ciberincidentes ocurridos en las plantas industriales, lo cual es imprescindible para que la dirección de la organización y las áreas de negocio sean conscientes de la magnitud del problema pudiendo así habilitar las herramientas necesarias para mejorar (por ejemplo, presupuesto).
- Del estudio se identifican dos factores principales que están acelerando la digitalización de la industria en Euskadi y como consecuencia de ello la necesidad de gestionar el riesgo tecnológico especialmente asociado con la ciberseguridad. En primer lugar, el escenario de regulación impulsado desde Europa, como la protección de infraestructuras críticas o más recientemente la directiva NIS, en el que las empresas vascas pueden verse afectadas por su actividad, determina el modo en que afrontan los retos planteados por los riesgos que afectan a sus sistemas de automatización y control industrial. En segundo lugar, la propia globalización, que provoca una mayor competencia del mercado, especialmente relevante en este estudio dado el perfil de las organizaciones que han decidido responder voluntariamente la encuesta.
- Destacan, además, en el estudio las aportaciones de aquellos sectores con mayor madurez en la adopción de nuevas tecnologías. Experiencia que les facilitará su proceso natural de acercamiento a la Industria 4.0 y, con él, una aproximación menos tímida a la ciberseguridad industrial. Promover foros intersectoriales o encuentros multiempresa podría favorecer que las organizaciones menos maduras (o menos internacionalizadas) vayan evolucionando su perfil, ya que en muchos casos empresas locales pequeñas suelen formar parte de la cadena de suministro de otras empresas locales internacionalizadas. El intercambio de experiencias puede ser muy beneficioso para el ecosistema.
- El mercado, las empresas y los proveedores de servicios en el ámbito industrial precisan de profesionales especializados en la ciberprotección de los entornos de producción industrial. Los esfuerzos en capacitación en ciberseguridad, en el conjunto de las empresas vascas estudiadas, siguen dedicándose, principalmente, a los departamentos de TI. Sería deseable ir aumentando el esfuerzo en capacitar y sensibilizar al resto de áreas de la empresa, especialmente las que operan y mantienen los sistemas de control.
- Las tecnologías de ciberseguridad más utilizadas en las redes de control de procesos siguen siendo las de uso habitual en las redes corporativas; aun cuando tales soluciones no sean siempre las óptimas para el entorno industrial. Por ello, se recomienda la adopción de medidas más específicas para dicho entorno, tales como la elaboración de listas blancas de aplicaciones (whitelisting, en inglés), los cortafuegos industriales, las pasarelas unidireccionales o los sistemas de prevención y detección de intrusiones (IDS) con características específicas para reconocer protocolos industriales, entre otras.
- El estudio sugiere que una de las razones principales para incorporar la ciberseguridad ha sido la mejora continua. Es este un dato muy significativo porque de ello se desprende que, al menos de manera implícita, se percibe la aplicación de ciberseguridad como un camino hacia las mejoras en la calidad, eficiencia y seguridad de los procesos.

Finalmente, como contexto de todas las conclusiones anteriores, cabe subrayar que una mayoría significativa de las organizaciones vascas encuestadas (de todos los sectores de la industria) tienen previsto abordar a lo largo de 2018 iniciativas de Ciberseguridad Industrial, lo que casi con toda seguridad implicará un aumento de los presupuestos destinados a esta materia y es esperable, aunque no es fácil de cuantificar, que se produzca una elevación del grado de madurez general.

glosario

- › Ciberseguridad Industrial 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, utilizando las perspectivas de personas, procesos y tecnologías
- › IDS Intrusión Detection Systems
- › IDPS Intrusion Detection and Prevention Systems
- › IPS Intrusion Prevention Systems
- › IEC International Electrotechnical Commission
- › ISA The International Society of Automation
- › ISO International Organization for Standardization
- › IT Information Technology
- › NERC CIP CIP Standards (Estándares de Protección de Infraestructura Críticas)
- › NIST National Institute of Standards and Technology
- › OT Operation Technology
- › SIEM Security information and event management
- › TO Tecnología de Operación (Automatización Industrial)
- › TI Tecnología de la Información



📍 Maiquez, 18 · 28009 MADRID
📞 +34 910 910 751
✉️ info@CCI-es.org
🌐 www.CCI-es.org
🌐 blog.CCI-es.org
🐦 @info_CCI
linkedin www.linkedin.com/in/centrociberseguridadindustrial/



📍 Parque Tecnológico de Álava
📞 +34 945 010 059
✉️ info@bcsc.eus
🌐 www.basquecybersecurity.eus
🐦 @basquecscentre
linkedin www.linkedin.com/company/basque-cybersecurity-centre/