CENTRO DE CIBERSEGURIDAD INDUSTRIAL

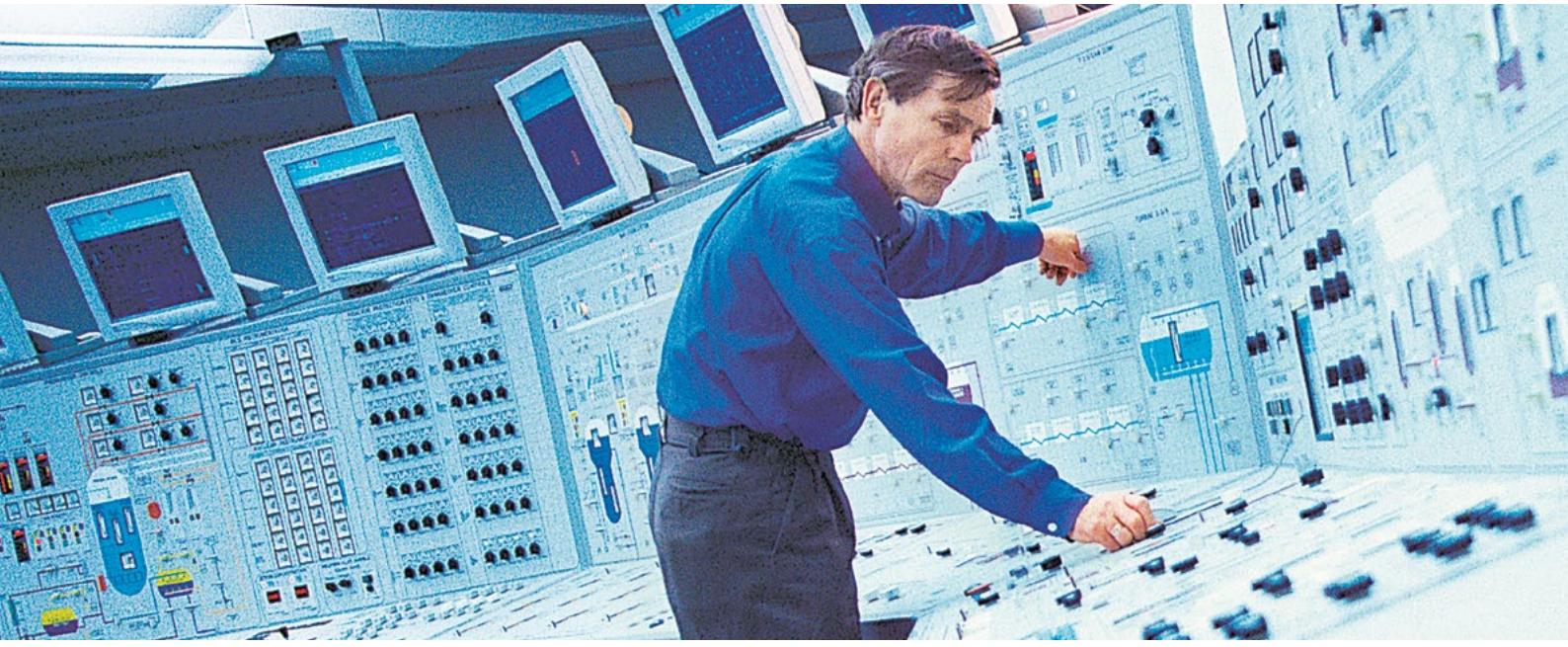

# Estudio sobre la Ciberseguridad Industrial en Colombia

Edición 2018

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 puntales 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: 978-84-942379-9-7
Segunda edición: abril de 2018



Maiquez, 18 · 28009 MADRID
+34 910 910 751
info@cci-es.org
www.cci-es.org
blog.cci-es.org
@info_cci

# Autores


- Susana Asensio
- Miguel García-Menéndez
- José Valiente
- Diego Zuluaga

# Patrocinadores del CCI

## Platinum

Eleven Paths

Telefónica

iHackLabs

## Gold

Check Point SOFTWARE TECHNOLOGIES LTD.

Cisco

InnoTec System Entelgy

Fortinet

paloalto NETWORKS

## Silver

Accenture Security

Capsa Food

dimension data

Govertis Advisory Services

CMC

Kaspersky Lab

S21sec

Siemens

Tecnicas Reunidas

Trend Micro

TSK Grupo

TÜVIT TÜV NORD GROUP

## Bronze

Atos

Eulen Seguridad

everis

gmv Innovating Solutions

Intermark it El valor del compromiso

Logitek

minsait by Indra

Nozomi Networks

oylo Trust Engineering

Phoenix Contact

S2 Grupo

sia

tecnalia Inspiring Business

Westcon Comstor Delivering Results Together

# Índice

# DESCRIPCIÓN DEL ESTUDIO

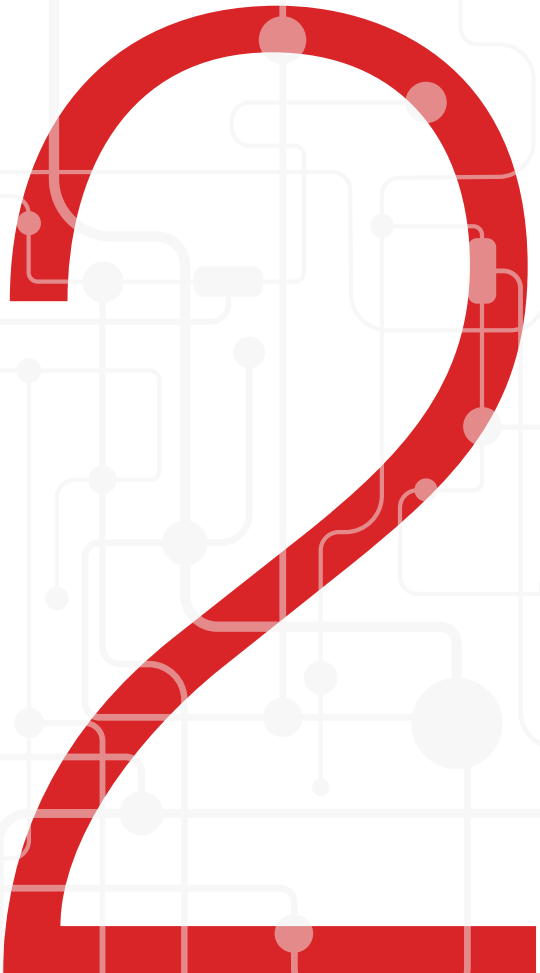
El estudio se ha realizado de forma *online*. Fue enviado por e-mail, con un formulario adjunto, a gestores de empresas colombianas. Durante el tiempo en el que el formulario estuvo abierto, desde octubre de 2017 hasta febrero de 2018, **35 empresas industriales** lo diligenciaron íntegramente.

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

La última sección incluye una comparativa de los resultados más significativos de los estudios realizados por CCI durante los periodos 2015-2016 (Edición 2016) y 2017-2018 (presente documento) en Colombia, con el objetivo de presentar la evolución y tendencias en el uso e implementación de la ciberseguridad industrial en las organizaciones colombianas.

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

# EMPRESAS ANALIZADAS



Los encuestados participantes en el estudio son los representantes de organizaciones pertenecientes a los sectores con más auge del país, aquellos que tienen mayor peso en la economía colombiana. La mayor parte de la muestra la ocupa el sector eléctrico, seguidas del sector de las tecnologías de la información. También han participado organizaciones del sistema financiero, y suministros: gas y petróleo, además de una breve representación de otros sectores, agua, administración pública y transporte (aeropuertos, puertos, tráfico, ...), entre otros.

## Sector de la organización a la que representa

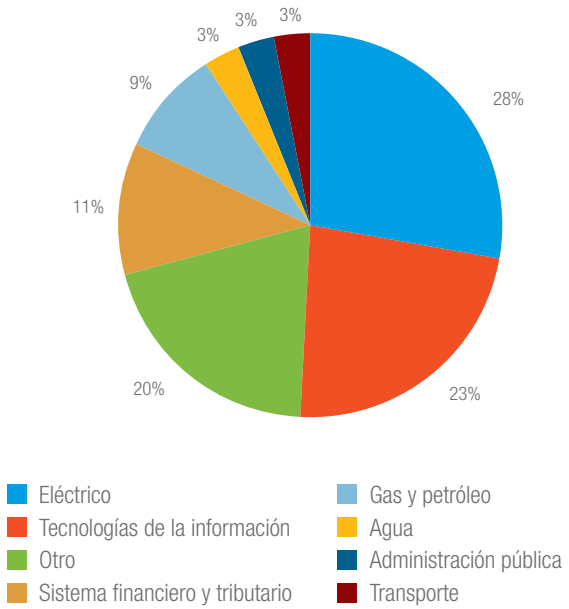



Gráfico 1 – Sectores representados en el estudio.

El estudio cuenta con el respaldo de una gran heterogeneidad de empresas, pertenecientes a un ecosistema global, con un alcance geográfico tanto nacional como internacional, debido a que la Ciberseguridad Industrial es fuertemente transversal, implicando el total de la variedad de sectores de la industria.

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 la Ciberseguridad Industrial en estos últimos años, no solo 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 colombiano.

## Número de empleados


Gráfico 2 – Número de empleados.

## Alcance geográfico


Gráfico 3 – Alcance geográfico.

## Facturación Global


Gráfico 4 – Facturación global.

En base a los datos obtenidos de número de empleados y facturación global, la mayoría de las empresas que han participado son grandes industrias colombianas y parte importante de las infraestructuras críticas del país, aunque solo un tímido 31% tiene presencia fuera de las fronteras del país. Este tipo empresas (grandes en contraposición a PYMES) son generalmente las más activas a nivel de protección de sus infraestructuras, bien por propia voluntad -mayor nivel de concienciación- o preocupación por requisitos legales debido a su naturaleza de infraestructura esencial para el adecuado funcionamiento del país.

# ORGANIZACIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

3

En esta sección del estudio, ha de tenerse en cuenta que la más que probable diferente estructura organizativa de las instituciones analizadas, puede determinar las diferentes atribuciones de responsabilidades, implicaciones y capacidades frente a la Ciberseguridad Industrial observadas.

## 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, entre aquellos que ya han definido la responsabilidad en materia de ciberseguridad, a disgregar dicha responsabilidad entre varias unidades organizativas de la empresa. Ninguna de las entidades encuestadas concentra dicho compromiso en un único departamento. Aunque el dato más preocupante que arroja el estudio es el alto número de organizaciones que aún no se han enfrentado a la realidad actual, y no han definido esta responsabilidad. En estos casos, la ciberseguridad no es una competencia asignada a ningún área en concreto de la organización, lo que supone que no se la está dotando del compromiso, presupuesto y mecanismos precisos para asegurar que se llevan a cabo las medidas necesarias.

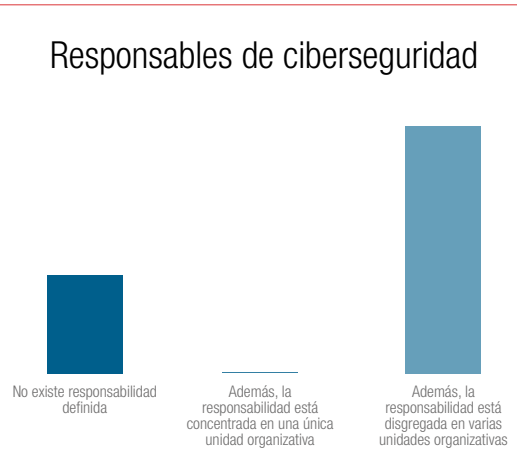



Gráfico 5 – Responsables de Ciberseguridad.

En lo que a unidades organizacionales responsables se refiere, gran parte de las entidades encuestadas (55,2%) asigna dicha tarea al área de seguridad de la información y/o seguridad lógica, enfocando estas acciones desde un punto de vista más cibernético que físico o asociado a procesos. Esto puede ser debido a la mayor madurez de estas áreas en materia de ciberseguridad, frente a las áreas técnicas de la operativa industrial, u otras.

En segundo lugar, aunque muy de cerca, en torno a un 48% de las respuestas obtenidas asignan dicha responsabilidad, a las áreas de Tecnologías de la Información corporativa (TI) y un significativo 31%, al CISO-Oficial de Seguridad Informática.

En otro rango de números, en torno al 20% en cada uno de los supuestos, se mueve el segmento de empresas que otorga esta responsabilidad a los departamentos más cercanos a la operativa de la organización, así seguridad física, operaciones, el CISO oficial de Seguridad en los SCI, y HSE (Riesgo Laboral y Medioambiental) se mueven en este rango.

Automatización de procesos apenas alcanza el 10%, dato que habla de la aún alejada realidad de los departamentos de automatización respecto a los temas de ciberseguridad en su entorno.

No obstante, no son todo malas noticias en esta esfera, puesto que, sin ser una unidad organizativa como tal, un gran número de encuestados ha marcado entre sus respuestas, la aplicación directa de esta responsabilidad sobre los hombros del CISO. Este gran paso hacia la normalización del trato de la disciplina de la ciberseguridad dentro de las organizaciones es la antesala a la capacidad de gestionar los riesgos cibernéticos como ya hace años se viene haciendo con el resto de riesgos (primordialmente físicos) de la organización. De esta forma, una organización madura a este respecto tendrá perfectamente definida la responsabilidad que ocupa la protección y resiliencia de sus activos, y al responsable(s) de la misma.

## Unidades organizaciones responsables

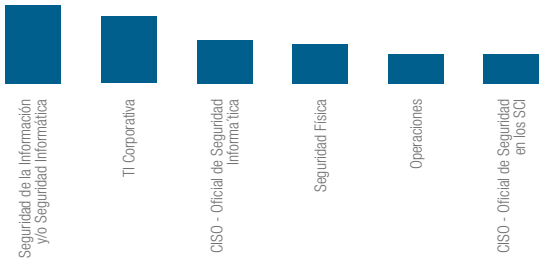



Gráfico 6 – Unidades organizacionales responsables.

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

En estrecha relación al grado de responsabilidad en la protección de los sistemas que controlan los procesos industriales, se observa como el área TI tiene, con diferencia, la mayor participación e implicación, seguido de las áreas de TO (Tecnologías de Operación), seguidos de las áreas de seguridad física, e ingeniería.

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

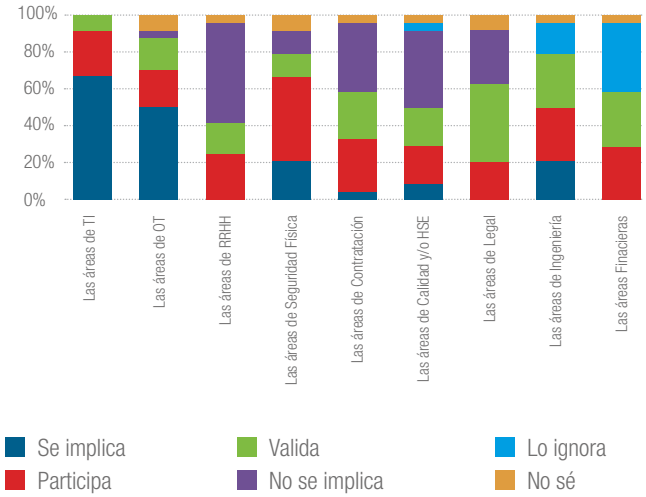



Gráfico 7 – Participación de las áreas de la organización

¿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 gestores de las empresas estudiadas (45,8%) se encuentran sensibilizados en un nivel considerado normal, frente a las normas y riesgos en redes industriales.

Por desgracia, un muy importante 33% de los gestores afirma estar muy poco sensibilizado frente a estos riesgos, lo que permite comprender la complejidad con la que trabajan, enfrentándose a importantes riesgos de continuidad y funcionamiento, sin el respaldo adecuado de la dirección; probablemente sin apoyo en la toma de decisiones, ni presupuesto suficiente para minimizar riesgo y daños. En este contexto, es imprescindible realizar un esfuerzo mayor de concienciación a nivel directivo, que ayude a garantizar la toma de conciencia del peligro al que está expuesta la continuidad de la organización.

Finalmente, en contraposición a lo anterior, un menor número de ellos (16%) considera el nivel de sensibilización bastante significativo. Deseamos que esta cifra siga incrementándose gradualmente en los próximos años.

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

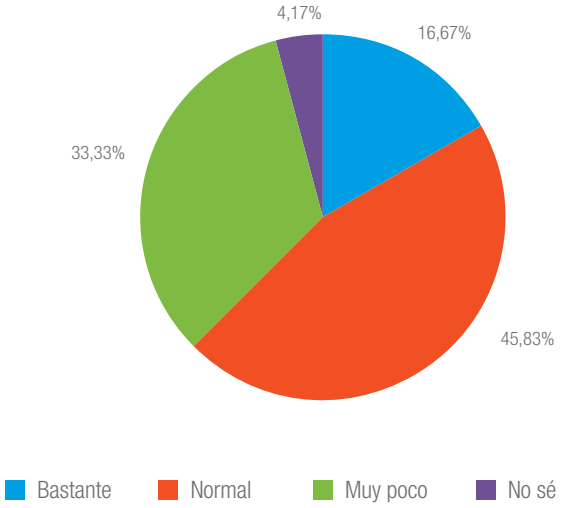



Gráfico 8 – Nivel de sensibilización de los responsables del negocio.

Estas cifras se verían incrementadas gracias a una intensa actividad de concienciación en las distintas jerarquías de la empresa tanto a nivel de dirección, como en todos aquellos empleados 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 nacionales jalonadas desde ministerios como el de las TIC y Defensa derivadas del Documento CONPES 3854 Política Nacional de Seguridad Digital en Colombia, e iniciativas sectoriales como las del Consejo Nacional de Operación del Sector eléctrico y las exigencias de las superintendencias como la de Industria y Comercio y la Financiera han comenzado a permear en las altas esferas empresariales y se espera que entren con fuerza en desarrollos de conciencia a todos los niveles organizacionales por lo menos inicialmente en las empresas públicas y las responsables de infraestructuras críticas. Esta acción de sensibilización o formación mínima en los conceptos de riesgo y medidas de protección general y en materia de ciberseguridad industrial debe ser diseñada específicamente para cada colectivo, de forma que, cada uno de ellos, pueda ver claramente las ventajas de su implementación, respecto a sus competencias y responsabilidades sobre los activos de la empresa.

El objetivo último de estos programas de concienciación debería ser contribuir a que el individuo asimile como una ventaja su compromiso con la ciberseguridad y deje de verlo como una exigencia de otros departamentos interesados en ello.

# 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 de datos, que relaciona el nivel de capacitación en esta disciplina, con las unidades organizacionales en las entidades participantes. La capacitación de las empresas en materia de Ciberseguridad Industrial, obviamente, varía según los departamentos. Aunque el motor económico de la empresa sea su área de producción -automatización y control-, las empresas industriales colombianas muestran mayor capacitación de 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.).

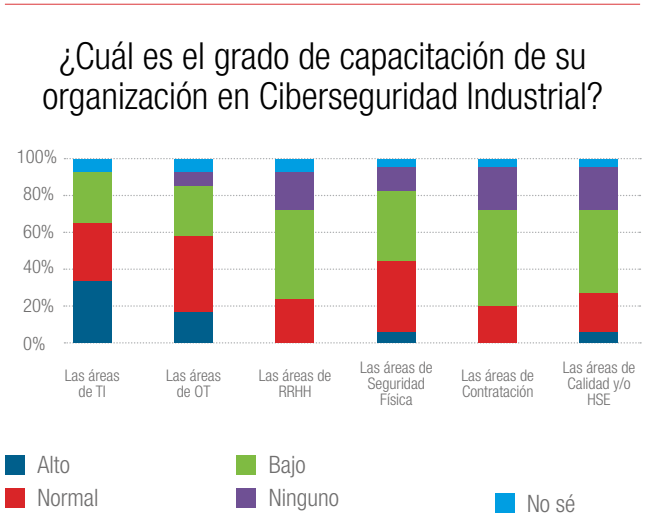



Gráfico 9 – Comparativa del nivel de capacitación de los equipos trabajo.

Es por tanto una tarea fundamental de los responsables de los procesos más vinculados con el negocio (OT) lograr un alto grado de resiliencia. Para lo cual requieren, ineludiblemente, capacitación específica frente a las amenazas que puedan entorpecer el correcto funcionamiento de los procesos de producción.

Fijándonos de nuevo en la gráfica, 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 (41%) de capacitación, y solo un 17% de los gestores considera que su equipo de automatización esté adecuadamente formado. Incluso un 7% 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.

# GESTIÓN DE LA 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 positivas y muestran una importante preocupación por analizar la situación real de exposición cibernética de la organización, tal vez ligada con los efectos de la política nacional de seguridad digital que basa su enfoque en la gestión adecuada de los riesgos.

Entre el conjunto de las evaluaciones realizadas, destaca con un 55% la referente a la capacidad organizativa, que incluye, entre otras variables, las políticas y procedimientos establecidos. Un casi 45% 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, al amparo de distintas normas y estándares como NERC-CIP, IEC62443, el SGCI de CCI (https://www.cci-es.org/sgci ), entre otras.

Aunque no excesivamente alto, pero si es significativo también el número de industrias (13,79%), que no han realizado ningún tipo de evaluación de riesgos, y no saben por tanto a las consecuencias que se enfrentan. En este caso, no en volumen, pero si en contexto, es un dato tremendamente preocupante, debido al tamaño y nivel crítico de las empresas que han respondido a este estudio.

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

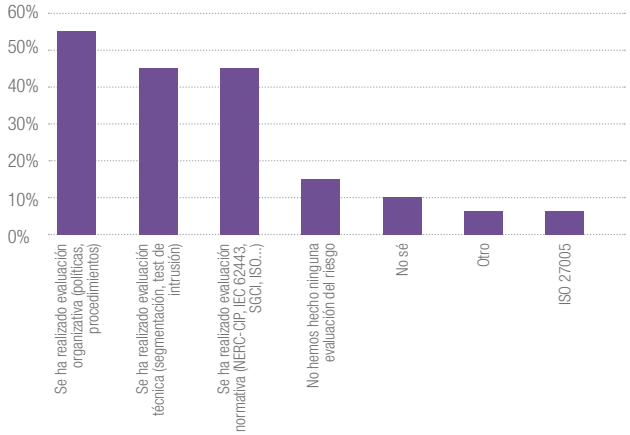



Gráfico 10 – Análisis de riesgos en sistemas de control y automatización industriales.

# GESTIÓN DE INCIDENCIAS DE SEGURIDAD

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

El 18% de las empresas estudiadas afirma tener un proceso de Gestión de Incidencias de Ciberseguridad Industrial desarrollado y en aplicación. En el 6,9% de las empresas este proceso no existe, y el 17,2% actúa de forma reactiva cuando ocurren incidencias de Seguridad. Por otro lado, el 28% de las empresas estudiadas afirma estar definiendo este proceso, el cual es necesario como se evidenció en los eventos de alto impacto global ocurridos en el 2017, como Wanacry y Petya, y en los sectores industriales afectados por los eventos como los apagones en Ucrania. Las afectaciones a sistemas de safety a plantas industriales en el mundo que cada vez son más frecuentes, así como del uso de los dispositivos IoT para ataques de negación de servicio masivamente, entre otros.

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

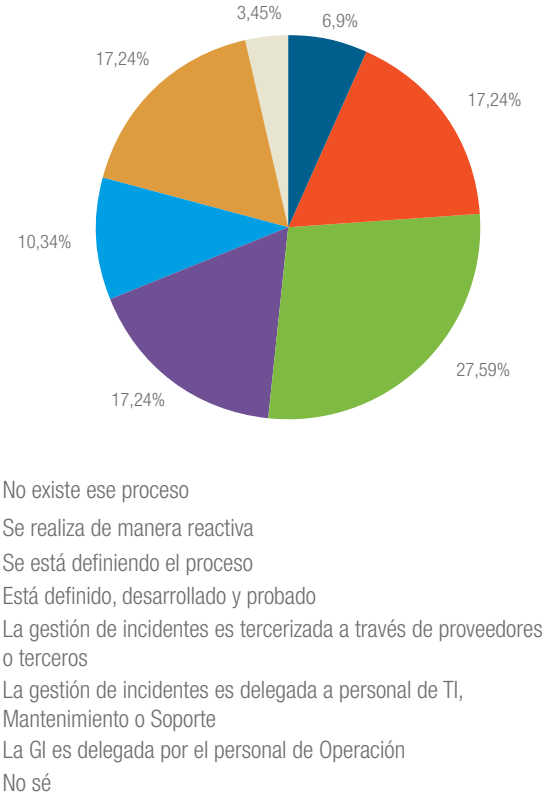



Gráfico 11 - Gestión de Incidencias de Seguridad Industrial.

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.

Deben existir una coordinación con los organismos externos adecuados -CERT y/o CSIRT- Como el ColCert, el Centro Cibernético Policial y Comando Conjunto Cibernético e incluir una hoja de ruta de recuperación de activos y resiliencia acorde a las necesidades específicas de cada entidad.

Las distintas iniciativas de intercambio de experiencias (tanto positivas como negativas), en los distintos aspectos de la ciberseguridad industrial -como la puesta en marcha por el CCI para su ecosistema-, permite a la comunidad obtener valiosa información que enriquece la definición efectiva de los distintos procesos relacionados con la ciberseguridad, y más en concreto, para el caso de la gestión de incidentes.

Respecto a los responsables de aplicar los planes definidos, el 17,24% de los encuestados manifiestan delegar la gestión de incidentes en el personal de TI, mantenimiento o soporte, pero en un número no muy alejado (10,34%), esa gestión es externalizada y delegada a un tercero, típicamente un proveedor especializado en servicios de ciberseguridad. Cabe destacar que en ningún caso la gestión de incidentes recae de forma específica sobre el personal de operación, lo que reafirma la necesidad de mayor implicación entre los departamentos responsables de la operativa de la organización.

## PLANIFICACIÓN DE INICIATIVAS DE CIBERSEGURIDAD INDUSTRIAL

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

En relación a la planificación de las iniciativas de Ciberseguridad Industrial, es llamativo observar una fuerte disparidad de actuaciones. Mientras que el 13% de las empresas reconocen seguir recomendaciones de una consultora externa, asciende al 23% los que afirman seguir recomendaciones de la operativa interna. Un 15% planifican, diseñan y ejecutan las iniciativas a lo largo del tiempo, y un 26% de las empresas industriales reconocen promover iniciativas bajo el motivo de la adecuación a directrices mínimas marcadas por legislación. Significativo es también el número de aquellas que solo actúan bajo reacción ante algún incidente (15%).

Es importante advertir que limitarse a mantener el grado de inversión en ciberseguridad en el mínimo que permite el cumplimiento legislativo implica que nuestros niveles de protección estarán muy por debajo del estándar necesario para hacer frente a los peligros actuales. Las leyes y normativas de los Estados son siempre lentas- lo cual es especialmente visible en temas técnicos complejos y alejados de los legisladores como la Ciberseguridad industrial- y la evolución tecnológica y de los ciberdelincentes muy rápida y con alta dedicación.

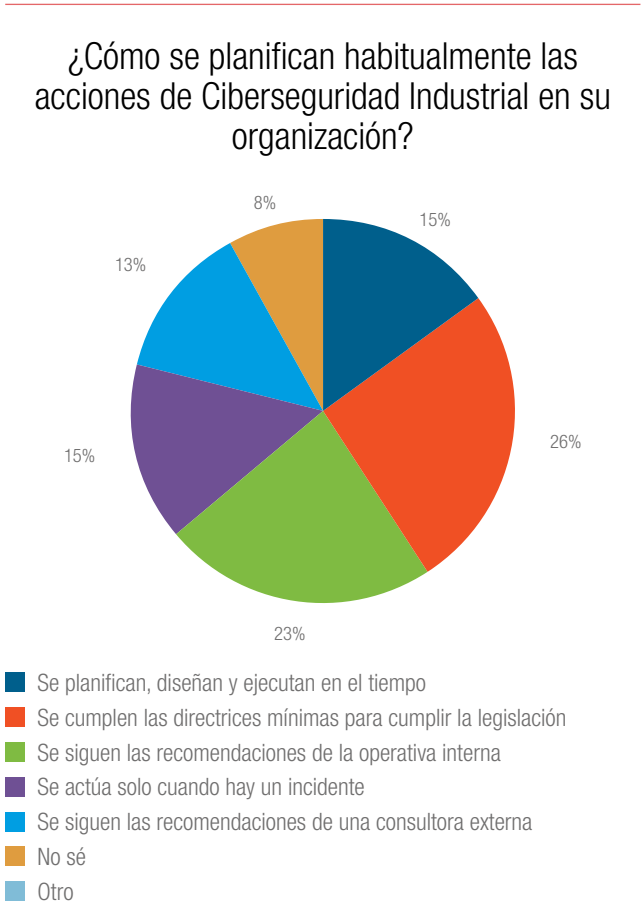



Gráfico 12 - Planificación de iniciativas de Ciberseguridad Industrial.

# ASPECTOS TÉCNICOS DE LA 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 muchos 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, poniendo en riesgo -si no se toman las medidas oportunas- la continuidad del negocio.

Más de la cuarta parte (31%) de las empresas industriales estudiadas afirman que existe una separación total entre sus redes, la corporativa y la industrial.

## ¿Están segmentadas y protegidas las redes en la organización?


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 la de automatización están segmentadas por un firewall (55%) o bien cuentan con distintos niveles de segmentación con varios dispositivos de filtrado (31%). Sin embargo, existe un muy preocupante 10% 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 aquellos que reconocían no haber realizado evaluación de riesgos, por lo que no cuentan con una percepción real del peligro que supone mantener sus redes -corporativa e industrial- 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 (35%) afirma tener dispositivos que están conectados a Internet de forma permanente. Desciende al 25% aquellos cuya conexión a internet es solo activada bajo demanda, y el mismo número 25%, el de los que manifiestan no tener ningún tipo de dispositivo en red abierta.

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

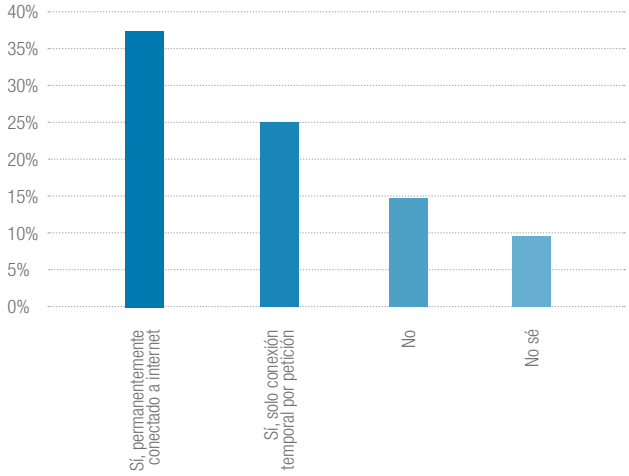



Gráfico 14 – Dispositivos de redes de automatización conectados a Internet.

Es preocupante el alto porcentaje de aquellos que manifiestan desconocer si disponen de dispositivos conectados a internet (15%) -especialmente si se trata de conexiones permanentes-, ya que el desconocimiento, en este caso, implica falta de protección, y por tanto fuerte vulnerabilidad de aquellos dispositivos a los que no se les esté inventariando como potencialmente en riesgo.

Actualmente existen distintas iniciativas que facilitan la detección de IPs expuestas -p.e. la bien conocida Shodan[1]-, herramientas que permiten el filtrado por diversos campos,

[1] https://www.shodan.io/ Shodan es el primer motor de búsqueda del mundo para dispositivos conectados a Internet.

de forma que el usuario, sin necesidad de grandes conocimientos en la materia, es capaz de detectar IPs vulnerables -conexiones a internet no identificadas- dentro de su organización. Por ello, es muy recomendable -no siendo excusa en este caso el presupuesto- realizar un estudio adecuado del nivel de exposición de nuestras redes y dispositivos, y de esta forma controlarlas y gestionarlas de forma correcta.

La existencia de sistemas de control industriales accesibles desde Internet, combinada con la escasa seguridad incorporada a los dispositivos industriales y el nivel crítico de muchos de los procesos controlados por estos dispositivos, hace que el riesgo de estos sistemas sea muy crítico e inaceptable para las organizaciones industriales.

¿Su red industrial posee accesos remotos?

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. En un mundo hiperconectado, la industria 4.0 es ya una industria altamente dependiente de las redes.

La gran mayoría de las empresas industriales estudiadas afirma que dispone de accesos remotos (75,8%). De todas ellas, el 24,1% tiene el acceso remoto permanentemente disponible para la conexión, mientras que en el 51,7% de estas empresas, los dispositivos de comunicación se conectan a demanda.

¿Tiene su red industrial accesos remotos?

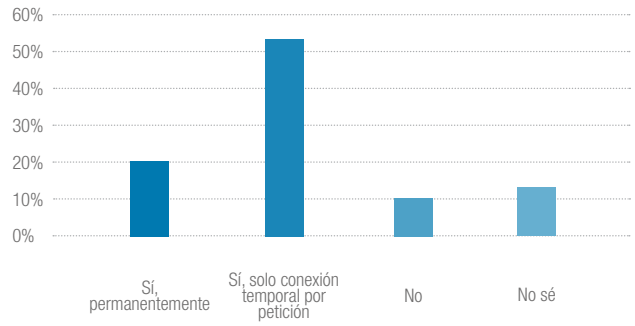



Gráfico 15 – Acceso remoto.

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 los mismos; así lo declara casi la mitad de los encuestados (47%). Mientras que un 36% accede a la red industrial para realizar labores de soporte y mantenimiento en remoto, bien a nivel del personal de empresa, o por terceras partes.

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

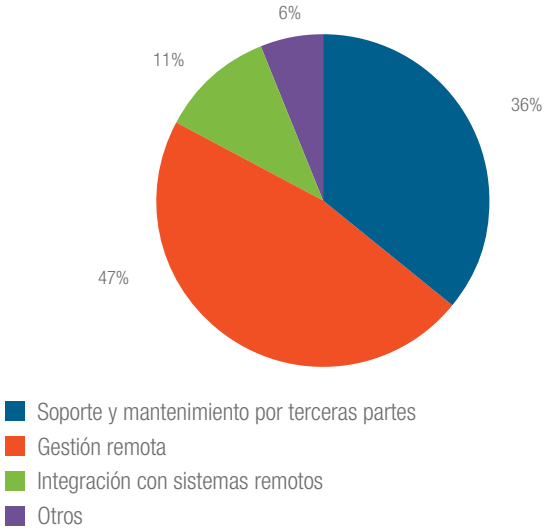



Gráfico 16 - Motivos para la utilización del acceso remoto.

# 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. La familia ISO 27001 lidera de lejos las preferencias de los entrevistados (71%). Son muy pocas las organizaciones industriales colombianas que no utilizan ninguna norma para implementar la Ciberseguridad Industrial (4,1%). Es muy destacable también que el 20% de las organizaciones encuestadas utilizan el estándar internacional IEC 62443 de seguridad en la automatización y control industrial.

## ¿Están utilizando normas y estándares en el ámbito industrial?

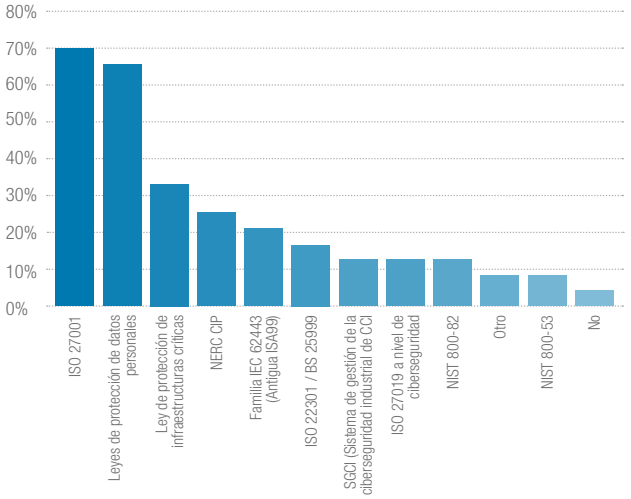



Gráfico 17 – Normas utilizadas en la Seguridad Cibernética Industrial.

De las normas específicas para la Ciberseguridad Industrial, aparecen las reglamentaciones sectoriales, como NERC CIP enfocada a la protección de infraestructuras críticas de sistemas de energía eléctrica, aspecto muy lógico por la participación elevada de este sector, ISO 27019 a nivel de ciberseguridad y la guía SGCI.

También encuentran fuerte cabida en el gráfico la aplicación de la Ley de Protección de Datos Personales (67%), y la futura y próxima Ley de Protección de Infraestructuras Críticas (33%).

# MEDIDAS DE CIBERSEGURIDAD INDUSTRIAL

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

Casi todas las empresas estudiadas 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 respaldo: backups o copias de seguridad, los antivirus, los firewalls convencionales y el cifrado de las comunicaciones.

También ocupan un lugar importante los IDS/IPS, la definición de políticas y procedimientos, la gestión de respuesta a incidentes, y la realización periódica de auditorías de seguridad internas.

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

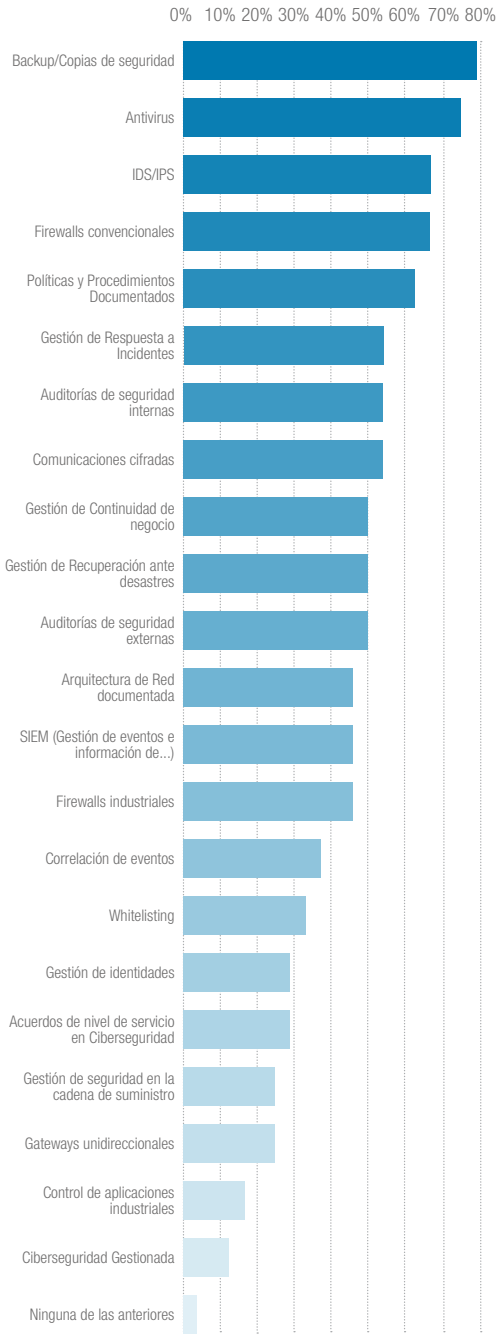



Gráfico 18 – Medidas de Seguridad Cibernética Industrial utilizadas.

Existen diversas medidas de ciberseguridad implantadas en las redes y sistemas industriales actualmente, pero no todas ellas son igual de eficaces respecto a lo esperado, ya que algunas, son aplicadas en estos entornos sin el criterio adecuado (provienen de entornos IT y no han sido adaptadas). Por ejemplo, el tráfico que soportan los entornos industriales tiene unas características específicas, que permiten 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 IT disminuyan en beneficio de las diseñadas específicamente para entornos OT, fruto de la adaptación de las soluciones IT a las necesidades y protocolos industriales. Así es el caso, de los firewalls industriales, frente a los convencionales, los cuales paulatinamente, irán ocupando mayor presencia en este gráfico hasta llegar a perder protagonismo.

# MERCADO DE LA CIBERSEGURIDAD INDUSTRIAL

# PREVISIÓN DE NUEVAS ACTIVIDADES DE CIBERSEGURIDAD INDUSTRIAL

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

Un determinante 83% de las empresas estudiadas prevé iniciar actividades de Ciberseguridad Industrial, y casi la mitad de ellas (46%) lo hará en el próximo año. Un 21% se encuentra ya en fase de implementación en los próximos 6 meses, contando por tanto con presupuesto específico asignado. Solamente el 17% 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?

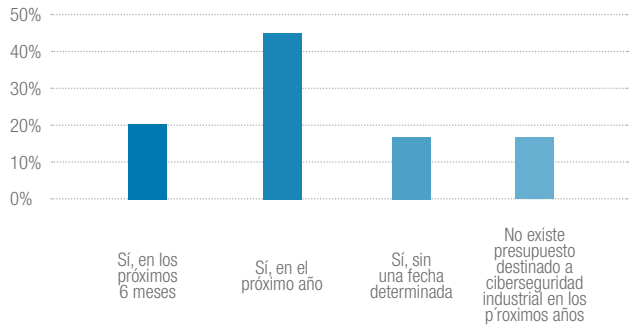



Gráfico 19 – Previsión de nuevas actividades en Ciberseguridad Industrial.

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 cada cliente. 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 estás acciones, en última instancia, no cuentan con la implicación y respaldo adecuados 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 para el sector. 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 la Escuela Profesional de Ciberseguridad Industrial[2].

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

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

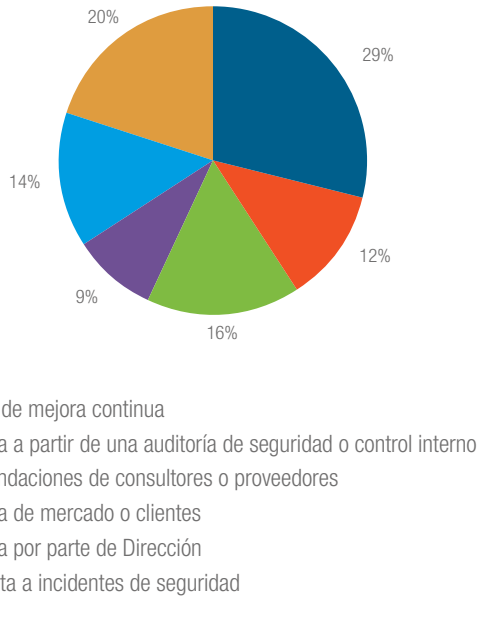



Gráfico 20 – Motivación para la ejecución de Proyectos de Ciberseguridad Industrial.

Las empresas encuestadas muestran una fuerte disparidad en lo que respecta a las motivaciones que las inducen a aplicar ciberseguridad industrial. Una de las principales motivaciones, la mejora continua (29%), es coherente con

[2] https://www.cci-es.org/escuela Escuela Profesional de Ciberseguridad Industrial del Centro de Ciberseguridad Industrial

el escenario actual, en el que las amenazas a los procesos industriales están cambiando debido a la introducción de componentes tecnológicos (principalmente la integración con tecnología de la información), que incorporan un riesgo para el cuál las industrias no están preparadas.

Asociado a esta misma razón, el 20% reconoce aplicar medidas como respuesta a incidentes de ciberseguridad, de nuevo como método imprescindible para adaptarse al nuevo entorno. Es significativa la mayor presencia de otros factores importantes en este contexto, como las exigencias por parte de Dirección, las auditorías internas, las recomendaciones de consultores o proveedores; y son las necesidades del mercado, lo cual denota un incremento de la madurez de este tema, que exige al mercado 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 (58%) consideran que la inversión en Ciberseguridad Industrial se incrementará, mientras que unánimemente, nadie ha considerado que disminuirá. Es también muy significativo (42%) el número de aquellos que consideran que el presupuesto actual será el vigente en un futuro próximo, pero considerando el estudio anterior, esto podría significar que se están manteniendo las partidas que ya han sido destinadas.

En su opinión ¿Cual será la evolución de cara al futuro en inversión de recursos humanos y presupuesto en Ciberseguridad Industrial?

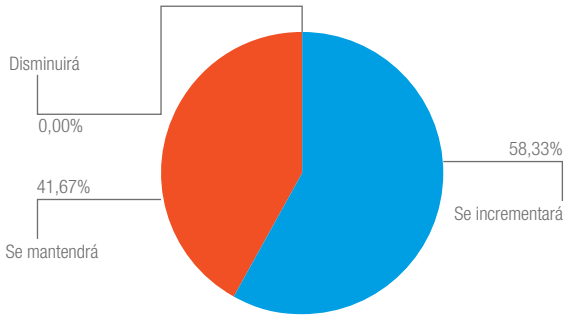



Gráfico 21 – Tendencia de las inversiones en Ciberseguridad Industrial.

# 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 casi un 20% de las empresas no considere requisitos de ciberseguridad en el diseño de sus nuevos proyectos. Sin duda, este escenario irá evolucionando a medida que aumente la concienciación de los equipos de automatización frente a la Ciberseguridad Industrial, o en aquellos casos en los que un incidente de ciberseguridad haga saltar las alarmas haciendo llegar su eco hasta las decisiones de Dirección, de forma que los presupuestos pasen a incorporar siempre 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?

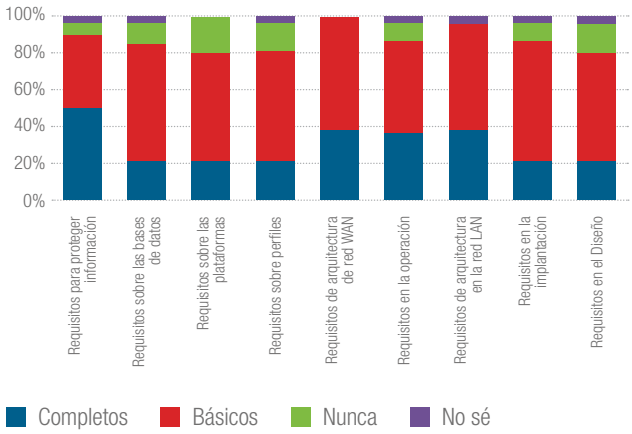



Gráfico 22 – Requisitos de Ciberseguridad Industrial en nuevos Proyectos.

# 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 el área de T.I. (71%) sobre quien previamente hemos visto recae la mayor implicación y participación en las tareas de ciberseguridad industrial. Con un 46%, el área de negocio es el también participe de la toma de decisiones en este ámbito, en no pocas organizaciones.

Solo un 20% 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 20% supone el número de encuestados que manifiestan que en su entidad, 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?

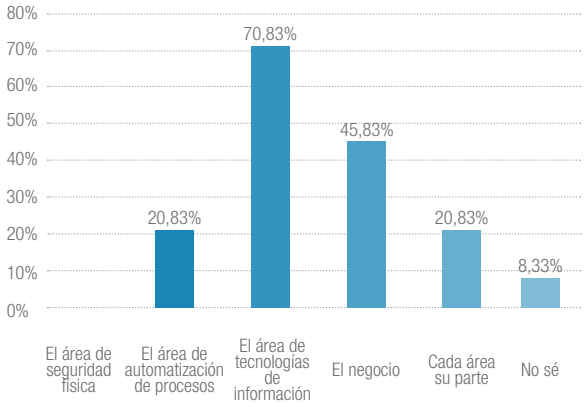



Gráfico 23 – Decisiones de contratación.

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

En cuanto al tipo de empresa proveedora de Ciberseguridad para empresas industriales, el estudio muestra que existe cierta inclinación por las empresas consultoras especializadas en ciberseguridad (54%), aunque también tienen amplia cabida entre los agentes identificados los fabricantes industriales con alianzas con especialistas en ciberseguridad (46%), seguido por las ingenierías o integradores industriales con sus propios recursos (37%) y los fabricantes de ciberseguridad (33%). .

¿Quienes son los proveedores de ciberseguridad en su organización?

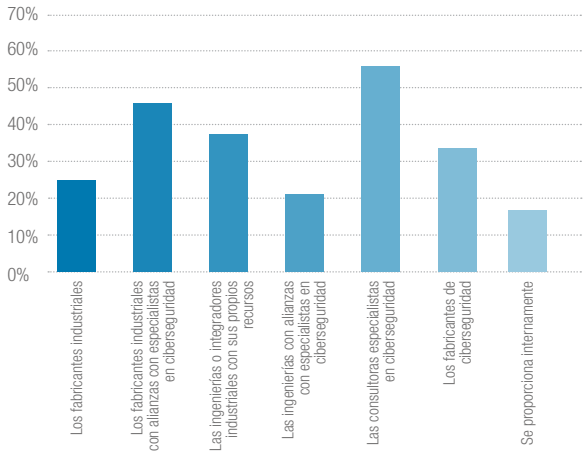



Gráfico 24 – Proveedores de Seguridad Cibernética Industrial.

# 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 encuestas también son conscientes de ello y por eso 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 (58%) o positiva (42%), y unánimemente, ninguna de las empresas niega 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, lo que las convierte en un criterio de valor a tener en cuenta en todo proceso de selección de personal y proveedores que presten servicios de Ciberseguridad Industrial. Por este motivo, CCI cuenta con su propio sistema de credenciales[3], 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.

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

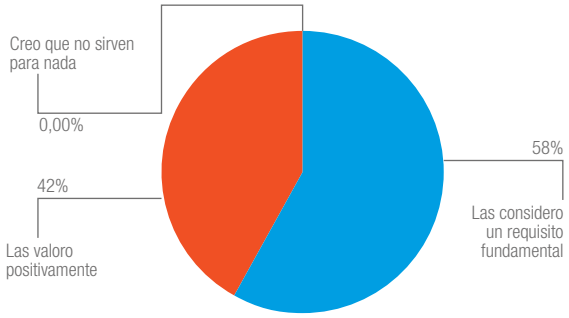



Gráfico 25 – Valoración de la importancia de las certificaciones.

[3] https://www.cci-es.org/credenciales 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 cíber" en el seno de sus organizaciones, o como eje central de su formación, y que demuestren un compromiso con el desarrollo de esta disciplina.

# EVOLUCIÓN DE LA CIBERSEGURIDAD INDUSTRIAL EN COLOMBIA

7

## COMPARATIVA DE RESULTADOS DE ESTUDIOS REALIZADOS POR CCI EN 2015-2016 FRENTE A 2017-2018

El Centro de Ciberseguridad Industrial realizó en 2015-2016 su primer Estudio de la Ciberseguridad Industrial en Colombia. Este documento presentó los resultados del estudio realizado a gestores de 36 empresas industriales colombianas, e incluía una interpretación de los mismos basada en el conocimiento y experiencia de sus redactores y de los participantes en el proceso de revisión.

Gracias a la comparativa de los datos recogidos en 2015-2016, frente a los resultados obtenidos en 2017-2018, es posible observar la evolución de los distintos aspectos de la ciberseguridad industrial en las organizaciones participantes.

En las siguientes líneas, se relacionan ambos periodos respecto a los aspectos más significativos del presente estudio.

## COMPARATIVA DE RESULTADOS DE ESTUDIOS REALIZADOS POR CCI EN 2015-2016 FRENTE A 2017-2018

Para ser consecuentes en la comparativa, es necesario inicialmente comprobar que ambos resultados pueden ser equiparables en lo que se refiere a caracterización de la población encuestada.

Tanto en el estudio de 2015-2016 como en presente de 2017-2018, la mayoría de las empresas participantes son grandes empresas colombianas (más de 500 empleados y más de 200M$ de facturación global), con fuerte presencia nacional, y pertenecientes a sectores críticos para el país, con mayor incidencia en ambos casos del sector eléctrico, tributario y financiero, y gas y petróleo.

La mayor diferencia se encuentra en la presencia más considerable del sector de las tecnologías de la información en el estudio de 2015-2016. Este hecho, puede hacer variar los resultados a la baja, puesto que se trata de un sector más evolucionado en materia de protección de sus sistemas, y por lo tanto, la situación global de la ciberseguridad en 2015-2016, pudo verse beneficiada -frente a 2017-2018-, por esa alta participación de empresas de un sector puntero en esta disciplina.

Es interesante analizar como otros sectores que no se veían a sí mismos como influenciados por tecnologías de control industrial como el Financiero y el de alimentación, han respondido ahora esta encuesta dándose cuenta que los sistemas de automatización han influido en general en los diferentes sectores actualmente en elementos claves para la seguridad de los activos, las personas y el medio ambiente como los sistemas de automatización de edificios y la entrada de componentes de Industria 4.0 e Internet de las Cosas.

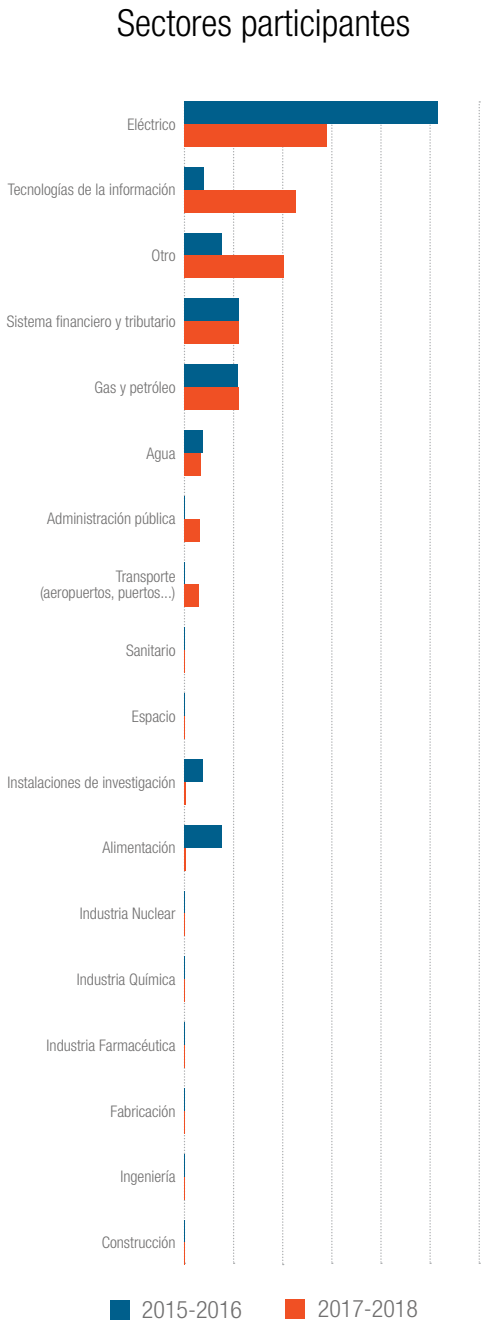



Gráfico 26 – Comparativa de sectores. Estudios 2015-2016 y 2017-2018.

# RESPONSABILIDAD DE PROTEGER LOS SISTEMAS QUE CONTROLAN LOS PROCESOS INDUSTRIALES

La responsabilidad de proteger los sistemas que controlan los procesos industriales no ha sufrido grandes variaciones en el tiempo respecto a los mayores protagonistas, pues éstos siguen siendo los departamentos más cercanos a entornos IT (Seguridad de la información, y TI corporativa). No obstante, sí existe un notable incremento en lo que se refiere al área de responsabilidad que asumen los entornos de procesos; en concreto seguridad física, operaciones y automatización de procesos aumentan notablemente su presencia en este gráfico. Además, la responsabilidad continúa siendo mayoritariamente disgregada en varias unidades organizativas.

Un dato que puede sorprender, y no precisamente en positivo, es que en el estudio de 2017-2018 existen organizaciones en las que la responsabilidad no ha sido aún asignada, cuando en 2015-2016 parecía que ya había sido superada dicha fase por todos los encuestados. Esta situación puede deberse, como comentábamos en la introducción de esta sección, a la mayor representación de diversos sectores en esta encuesta y a la mayor presencia de empresas del sector de las telecomunicaciones en el estudio de 2015-2016, empresas con mayor madurez respecto a la aplicación de ciberseguridad.

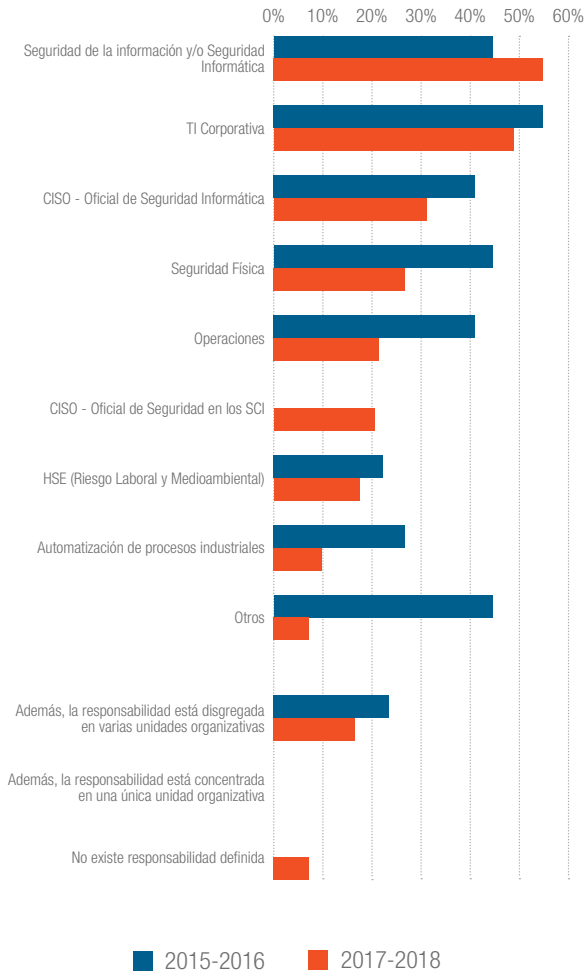



Gráfico 27 – Comparativa de Responsables de Ciberseguridad. Estudios 2015-2016 y 2017-2018.

# GRADO DE CAPACITACIÓN POR UNIDADES ORGANIZATIVAS

La capacitación de los profesionales con competencias en materia de ciberseguridad industrial, por unidades organizativas, ha sufrido una leve mejora en las áreas TI y OT, pero en el resto de las áreas, los encuestados, consideran que sus departamentos tienen mayormente una carencia de formación y/o experiencia entre sus empleados. Este dato puede ser motivado por la mayor madurez en este aspecto entre los propios encuestados, quienes, teniendo mejor conocimiento de la problemática, son más exigentes, críticos y rigurosos a la hora de emitir sus valoraciones respecto a la capacitación real de las distintas áreas de la organización, notándose el resultado del desarrollo de políticas públicas y emprendimientos privados en la materia que han ayudado a mejorar el entorno de conocimientos y entendimiento de las necesidades reales.

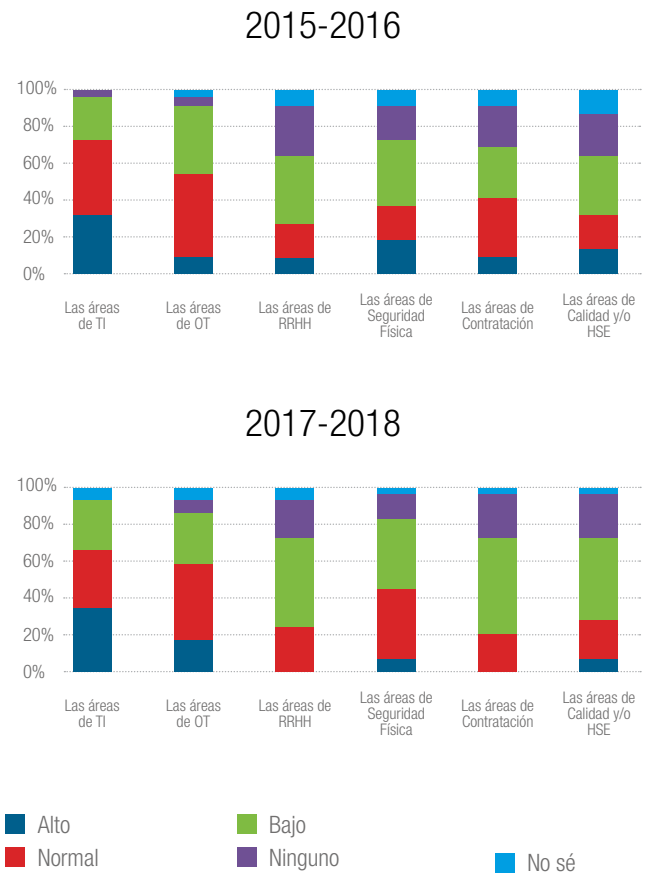



Gráfico 28 – Comparativa capacitación por áreas. Estudios 2015-2016 y 2017-2018.

# PROCESO DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD EN EL ÁMBITO INDUSTRIAL DE LAS ORGANIZACIONES

La evolución de la gestión de incidentes en las organizaciones colombianas, en general, habla de cierta madurez de los procesos. Ha disminuido considerablementeel el porcentage de aquellas en las que aún no se ha definido el proceso, e incrementado, consecuentemente, aquellas que ya tienen estas acciones definidas, desarrolladas y probadas, esto tambien se entiende como consecuencia de una mayor conciencia de la posibilidad e impactos de los mismos debido a los grandes incidentes globales vividos en los años anteriores que lograron un mayor entendimiento por parte de la dirección y los responsables como se ve en la evolucion de la respuesta sobre motivaciones para los proyectos de ciberseguridad industrial.

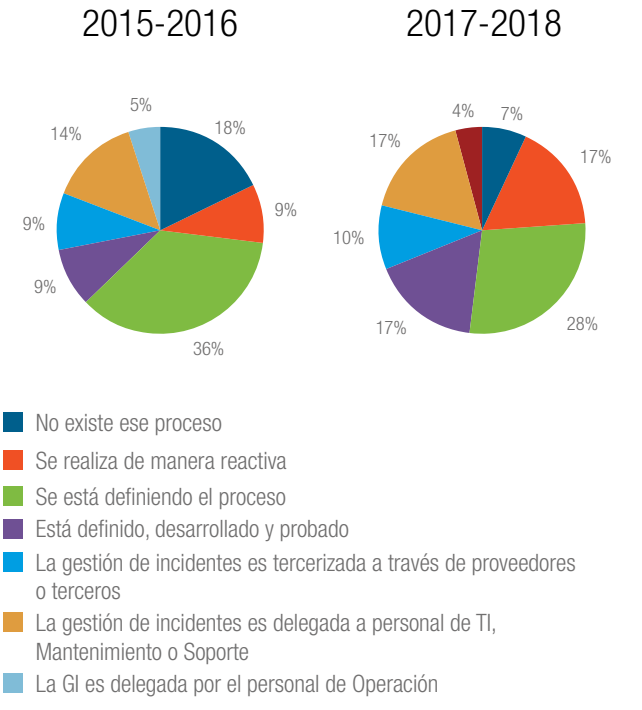



Gráfico 29 - Comparativa gestión de incidentes. Estudios 2015-2016 y 2017-2018.

# MEDIDAS DE CIBERSEGURIDAD IMPLANTADAS EN LA ORGANIZACIÓN EN EL ÁMBITO INDUSTRIAL

Las medidas de ciberseguridad que han declarado tener implementadas los encuestados en ambos periodos han sufrido en muchos casos una fuerte variación respecto a su incidencia. No necesariamente debemos tomar la siguiente tabla como tendencia en un proceso natural de desarrollo y madurez, ya que las diferencias pueden ser también debidas a los distintos sectores participantes en ambos estudios, así como a las diferencias organizacionales -a nivel interno y/o de políticas de contratación- de las empresas participantes.

## Medidas de ciberseguridad implantadas

| | 2015-2016 | 2017-2018 |
|---|---|---|
| Acuerdos de nivel de servicio en Ciberseguridad | 0,00% | 29,17% |
| Antivirus | 70,60% | 75,00% |
| Arquitectura de Red documentada | 64,70% | 45,83% |
| Auditorías de seguridad externas | 52,90% | 50,00% |
| Auditorías de seguridad internas | 70,60% | 54,17% |
| Backup/Copias de seguridad | 70,60% | 79,17% |
| Ciberseguridad Gestionada | 5,90% | 12,50% |
| Comunicaciones cifradas | 41,20% | 54,17% |
| Control de aplicaciones industriales | 17,60% | 16,67% |
| Correlación de eventos | 23,50% | 37,50% |
| Firewalls convencionales | 70,60% | 66,67% |
| Firewalls industriales | 52,90% | 45,83% |
| Gateways unidireccionales | 11,80% | 25,00% |
| Gestión de Continuidad de negocio | 41,20% | 50,00% |
| Gestión de identidades | 23,50% | 29,17% |
| Gestión de Recuperación ante desastres | 29,40% | 50,00% |
| Gestión de Respuesta a Incidentes | 35,30% | 54,17% |
| Gestión de seguridad en la cadena de suministro | 17,60% | 25,00% |
| IDS/IPS | 52,90% | 66,67% |
| Políticas y Procedimientos Documentados | 52,90% | 62,50% |
| SIEM (Gestión de eventos e información de ciberseguridad) | 29,40% | 45,83% |
| Whitelisting | 23,50% | 33,33% |
| Ninguna de las anteriores | 0,00% | 4,17% |

Tabla 1 – Medidas de ciberseguridad implantadas. Comparativa 2015-2016 y 2017-2018.

# NIVEL DE CONCIENCIACIÓN

En 2017-2018 mejora levemente el número de aquellos que consideran que la concienciación de sus responsables de negocio es bastante buena, mientras que desciende el número de aquellos que la consideran normal.

## Nivel de concienciación

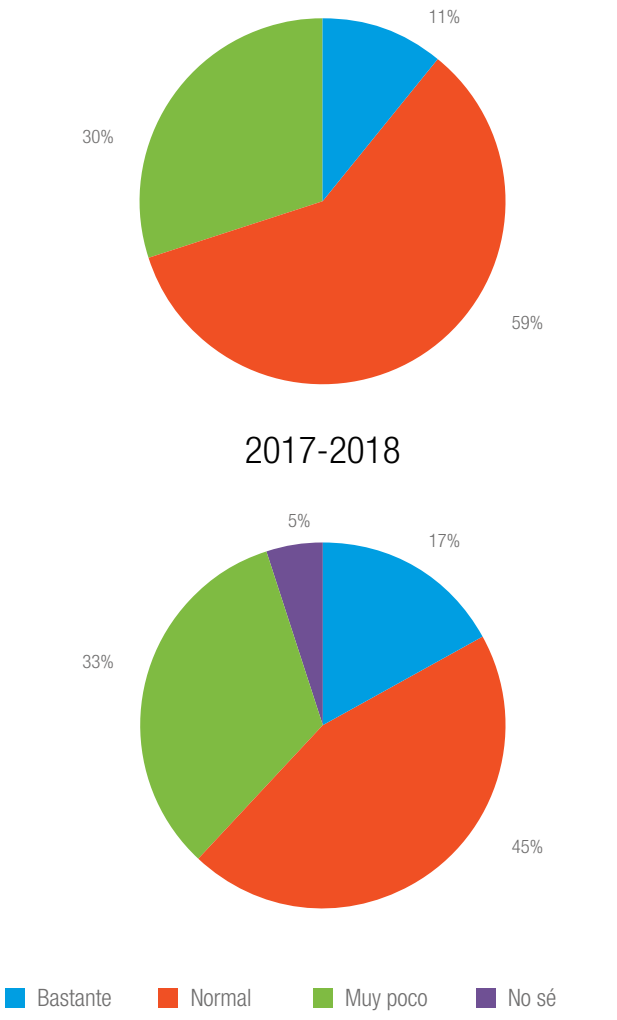



Gráfico 30 – Comparativa nivel de concienciación. Estudios 2015-2016 y 2017-2018.

# MOTIVOS PARA INCORPORAR CIBERSEGURIDAD EN EL ÁMBITO INDUSTRIAL

Las mayores diferencias que se producen entre periodos, a la hora de declarar las motivaciones que empujan a las organizaciones industriales a ejecutar proyectos e implantar soluciones de ciberseguridad, se dan entre aquellos que declaran que su principal motivación es la respuesta a incidentes, con un claro aumento -motivados probablemente, por las últimas oleadas de ataques cibernéticos a nivel mundial-, y el descenso de la exigencia por parte de auditorías de seguridad o control interno.

Motivos para incorporar ciberseguridad en el ámbito industrial

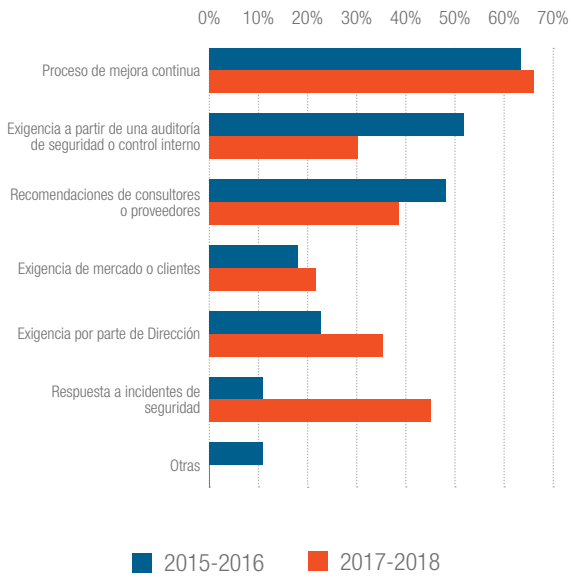



Gráfico 31 – Comparativa motivaciones de implantación. Estudios 2015-2016 y 2017-2018.

# EVOLUCIÓN DE LA INVERSIÓN EN CIBERSEGURIDAD EN EL ÁMBITO INDUSTRIAL

Se detecta una tendencia a mantener las mejoras que se proyectaban desde el primer estudio realizado por el CCI o mejorar las inversiones en recursos humanos y presupuestales para contrarrestar los riesgos en temas de Ciberseguridad Industrial, lo que evidencia lo que reiterativamente se ha logrado encontrar en este estudio. Cada vez más las empresas son conscientes del riesgo y que la administración del mismo demanda recursos capacitados, procesos adecuados y tecnologías especializadas que se deben desplegar en proyectos que consideren las particularidades de los entornos industriales.

En su opinión ¿Cual será la evolución de cara al futuro en inversión de recursos humanos y presupuesto en Ciberseguridad Industrial?

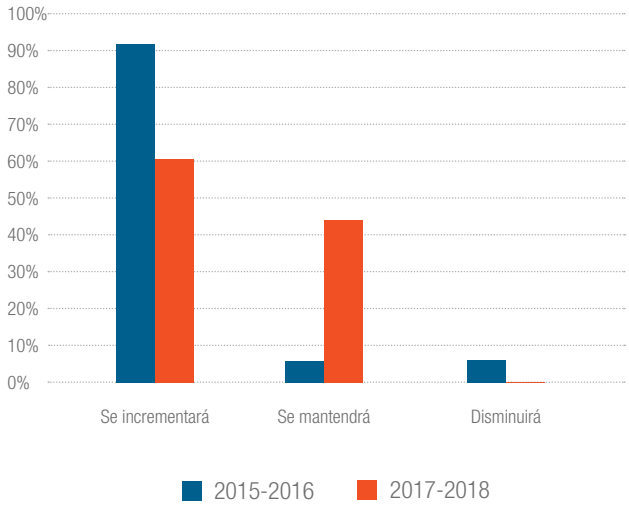
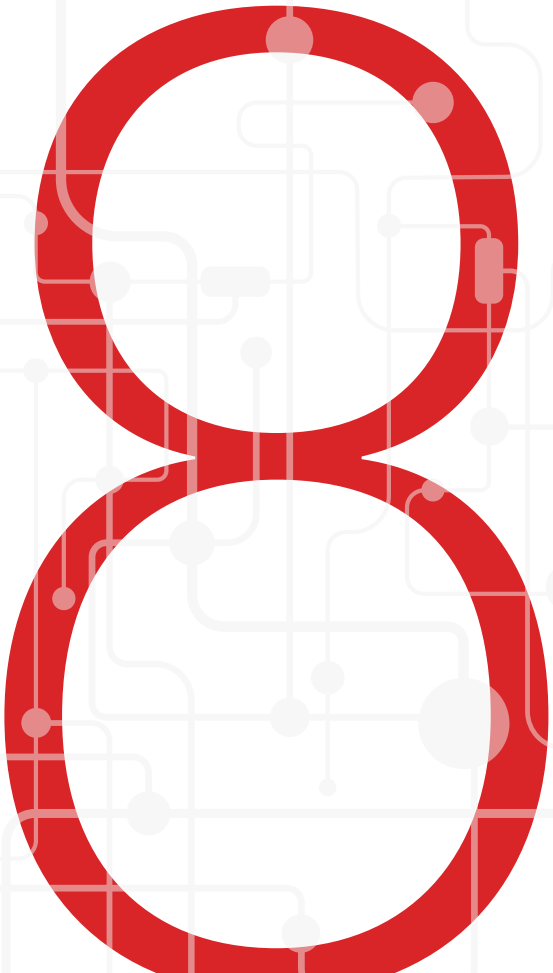



Gráfico 32 – Comparativa motivaciones de implantación. Estudios 2015-2016 y 2017-2018.

# CONCLUSIONES



- El contexto socioeconómico y regulatorio en el que las empresas colombianas desarrollan su actividad determina el modo en que afrontan los retos planteados por la inseguridad que puede afectar a sus sistemas de automatización y control industrial. Pero también la globalización, que provoca una mayor competencia del mercado, está obligando a la industria en Colombia a una transformación digital y la necesidad de gestionar el riesgo tecnológico especialmente el asociado con la ciberseguridad .
- 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.
- 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 colombianas estudiadas, siguen dedicándose, principalmente, a los departamentos de TI, sin considerar adecuadamente el resto de áreas de la empresa.
- Eso es motivo, asimismo, de que las tecnologías de ciberseguridad más utilizadas en las redes de control de procesos sigan 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 (IDPS) con características específicas para reconocer protocolos industriales, entre otras.
- Es preciso elevar el nivel de concienciación frente a la necesidad y las implicaciones de la Ciberseguridad Industrial. No obstante, aún se aprecian reticencias a la hora de reconocer y notificar los impactos derivados de ciberincidentes ocurridos en las plantas industriales; a diferencias de lo que ocurre en otros países en los cuales se dispone, incluso, de bases de datos específicas, y compartidas, al menos sectorialmente, con información de incidentes de Ciberseguridad Industrial.
- La participación de empresas del sistema financiero y tributario, y de tecnologías de la información, en el presente estudio permite concluir su mayor nivel de sensibilización frente a muchas de las cuestiones planteadas, donde el marco normativo y la madurez de estos dos sectores están guiando en muchos aspectos al resto.
- Adicionalmente, otra razón que justifica la necesidad de contar con marcos de referencia que ayuden a las organizaciones a afrontar los retos en este campo es la disparidad de estrategias de incorporación de la Ciberseguridad Industrial que pueden observarse entre diferentes empresas y sectores.
- Es muy significativo que una de las razones principales para incorporar la ciberseguridad haya sido la respuesta a incidentes, lo cual indica que se han producido en los últimos años incidentes de impacto considerable que están obligando a adoptar medidas de respuesta.
- Finalmente, y confirmando lo anterior, cabe subrayar que muchas organizaciones colombianas de todos los sectores de la industria tienen previsto abordar, a lo largo del presente año, iniciativas de Ciberseguridad Industrial, lo que implicará un aumento de los presupuestos destinados a esta materia.

# GLOSARIO

9

| | |
|---|---|
| › 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. |
| › T.O. | Tecnología de Operación (Automatización Industrial). |
| › T.I. | 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