ESTADO DE PREPARACIÓN EN CIBERSEGURIDAD DEL SECTOR ELÉCTRICO EN AMÉRICA LATINA

Diagnóstico, recomendaciones y guía de buenas prácticas

BID

ESTADO DE PREPARACIÓN
EN CIBERSEGURIDAD DEL SECTOR ELÉCTRICO
EN AMÉRICA LATINA

Diagnóstico, recomendaciones y guía de buenas prácticas

BID

cier
COMISIÓN DE INTEGRACIÓN
ENERGÉTICA REGIONAL

Contribución Técnica:

GOBERTIS
Advisory Services

Catalogación en la fuente proporcionada por la Biblioteca Felipe Herrera del Banco Interamericano de Desarrollo

Barrero, Vladimir.

Estado de preparación en ciberseguridad del sector eléctrico en América Latina / Vladimir Barrero, Oscar Bou; editores, Juan Roberto Paredes, Miguel Porrúa.

p. cm. — (Monografía del BID ; 802)

Incluye referencias bibliográficas.

1. Electric power systems-Security measures-Latin America. 2. Infrastructure (Economics)-Security measures-Latin America. 3. Computer security-Latin America. I. Bou, Oscar. II. Paredes, Juan Roberto, editor. III. Porrúa, Miguel, editor. IV. Banco Interamericano de Desarrollo. División de Energía. V. Banco Interamericano de Desarrollo. División de Innovación para Servir al Ciudadano. VI. Título. VII. Serie.

IDB-MG-802

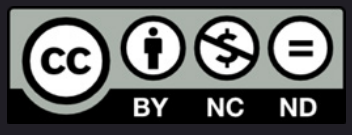
Códigos JEL: F50, L94, L96, O25
Palabras clave: ciberseguridad, seguridad industrial, sector eléctrico, internet, infraestructura crítica

AGRADECIMIENTOS

Esta publicación es un trabajo conjunto entre las Divisiones de Energía (INE/ENE) y de Innovación para Servir al Ciudadano (IFD/ICS) del Banco Interamericano de Desarrollo (BID) y la colaboración de la Comisión de Integración Energética Regional (CIER). Se realizó bajo la supervisión de Juan Paredes, especialista senior de la División de Energía y Ariel Nowersztern y Darío Kagelmacher por parte de la División de Innovación para Servir al Ciudadano. Se agradece de manera especial a las empresas eléctricas de América Latina que contribuyeron a la elaboración de este estudio, en particular al grupo de trabajo de ciberseguridad de la CIER y los expertos que aportaron valiosos comentarios y recomendaciones, Diego Andrés Zuluaga (ISAGEN), Sigifredo Hernández (CELSIA), Wilson Castillo (ISA), Jose Ignacio Ramírez (EPM), Rubén Darío Villa (XM), Fabio Reis Cortes (ONS) y Luis Enrique González (UT). También un agradecimiento al equipo de la CIER que apoyó el Taller Regional de Ciberseguridad realizado en 2018 en Montevideo, Uruguay, liderado por Jose Vicente Camargo.

Se agradece también a los dos equipos de consultores involucrados en el estudio: Scadasudo (Israel), encabezado por Yigal Goweta, por el diseño y realización de la encuesta de diagnóstico cuyos resultados y recomendaciones se reflejan en este reporte; y Govertis (España, Colombia), con Oscar Bou Bou y Vladimir Barrero Castro. Finalmente, un agradecimiento especial al Gobierno de Israel por su generoso apoyo a la publicación.

Edición Gráfica:
PUNTOAPARTE
Dirección de arte:
Andrés Álvarez
Diagramación:
Carmen Villegas
Paula Romero Echeverry



contenido

TABLA DE ILUSTRACIONES

PRÓLOGO

El extraordinario avance de la digitalización en el sector energético lo hace cada vez más sensible a los riesgos relacionados con ciberataques. Esta amenaza tiene el potencial de afectar gravemente las operaciones de las redes eléctricas. A pesar de que, en los últimos años, ha habido problemas de vulnerabilidad tecnológica, dirigidos específicamente al sector energético, el nivel de resiliencia de los sistemas de energía a estos ataques cibernéticos no puede ser evaluado simplemente desde la perspectiva de la debilidad física de la red. Por el contrario, se requiere de un profundo trabajo de diseminación de conocimiento y concienciación de los trabajadores a todo nivel de las organizaciones del sector sobre ciberseguridad y los sistemas de seguridad requeridos para prevenir ciberataques.

En las empresas del sector energético de la región latinoamericana el conocimiento sobre ciberseguridad comienza a desarrollarse. El Banco Interamericano de Desarrollo junto con la Comisión de Integración Energética Regional – CIER, aunaron esfuerzos para incrementar el conocimiento de lo que significa la ciberseguridad en las empresas del sector. En este sentido, se desarrolló el primer estudio regional sobre CIBERSEGURIDAD en los sistemas eléctricos de Latinoamérica, con el propósito de evaluar los riesgos y el estado de preparación de la ciberseguridad en las compañías eléctricas de América Latina y así intentar mejorar la capacidad de recursos humanos en este campo.

El estudio implicó diseñar un plan que comprendía realizar un diagnóstico, por medio de una encuesta digital, diseñada por el BID y bajo la coordinación técnica del Grupo de Trabajo específico de CIER. El mismo contó con información base de una muestra de 43 empresas en la región, dedicadas a los negocios de Generación, Transmisión, Distribución de energía eléctrica y de los Operadores Nacionales de los sistemas eléctricos.

De manera complementaria se realizó el Taller "CIBERSEGURIDAD en el Sector Eléctrico en ALC" organizado por el Banco Interamericano de Desarrollo (BID) junto a CIER en la ciudad de Montevideo, República Oriental del Uruguay. El motivo de tal actividad fue discutir los resultados y conocer la realidad de los riesgos sobre los sistemas eléctricos y la respuesta desde el punto de vista regulatorio y empresarial que se está implementando.

Este primer estudio de ciberseguridad del sector eléctrico de la región se convierte en un referente para comprender el estado y las acciones que deben ser desarrolladas por los diferentes países y empresas, con el fin de lograr la resiliencia frente a los crecientes y complejos ataques cibernéticos que se vienen presentando. Además, sirve como punto de partida para la definición de planes de acción y futuros estudios, a la vez que muestra la necesidad de construir conjuntamente un ecosistema de ciberseguridad que apoye a los diferentes actores para fortalecer la seguridad y confiabilidad del servicio esencial de energía eléctrica.

Los resultados nos llaman a establecer medidas de dirección, no sólo nacionales sino regionales, que generen conciencia y estandaricen buenas prácticas a través de los diferentes países para hacer frente al riesgo cibernético de manera adecuada. Como acción de corto plazo, CIER está estructurando un grupo regional de expertos en ciberseguridad de sistemas eléctricos que lidere el fortalecimiento de este sector y brinde herramientas que agilicen la construcción de un entorno confiable de operaciones del sector eléctrico en la región.

Lea Gimenez
Jefe División de Innovación
para Servir al Ciudadano BID

Ariel Yepez
Jefe División de Energía BID

Tulio Alves
Director Ejecutivo CIER

01 INTRODUCCIÓN

El presente informe describe el nivel actual de madurez de la ciberseguridad en la Industria de Energía Eléctrica en América Latina y el Caribe (ALC) a partir de las encuestas realizadas a diferentes actores del sector, agrupados en las categorías de generación, transmisión, distribución y operación (o una combinación de ellos) para el sistema eléctrico de la región. Asimismo, del análisis de las respuestas se extraen conclusiones y recomendaciones con el objetivo de ofrecer pautas de mejora en la ciberseguridad de estos sistemas e infraestructuras.

Los **hallazgos** encontrados en el estudio se basan en la **encuesta respondida por 43 empresas** de toda la cadena de suministro de la **electricidad**

Para su elaboración se ha contado con el apoyo y gestión de la Comisión de Integración Energética Regional-CIER y su Grupo de Trabajo de Operadores & Administradores de Mercado para concretar la participación de las empresas del sector eléctrico latinoamericano tanto en el diligenciamiento de la encuesta como en la revisión de documentos y realización del taller sobre "CIBERSEGURIDAD en el Sector Eléctrico en ALC". En este taller, además de analizar los primeros resultados de la encuesta y la problemática del riesgo cibernético, **se intercambiaron prácticas y experiencias directas de las empresas y operadores de sistema.** La encuesta fue respondida por 43 empresas del subsector eléctrico de la región, dirigida a los directores de seguridad de la información (CISO) y a los Ingenieros Superiores de Control de toda la cadena de suministro de electricidad, incluida la generación, transmisión, distribución y operación del sistema en la región . Se realizaron también entrevistas individuales con 7 empresas seleccionadas realizadas por la consultora SCADASUDO de Israel.

Este informe analiza tanto los resultados cualitativos como cuantitativos, detallando y analizando los resultados obtenidos y considerando los siguientes dominios de seguridad:

- **Gobernanza de la seguridad**
- **Gestión de la seguridad lógica**
- **Gestión de las comunicaciones**
- **Gestión de la cadena de suministro**

Uno de los **objetivos del estudio** es proporcionar recomendaciones a los **responsables** de establecer **políticas y estrategias de seguridad** en los estados **de la región**

Se proporciona también una visión general de las características de la ciberprotección en los entornos de automatización y control, en concreto en su aplicación al sector de la energía eléctrica, y las diferencias respecto a los escenarios de protección de la seguridad en entornos de Tecnologías de la Información (TI), con respecto a los que existen diferencias y singularidades relevantes. A modo de ejemplo, si consideramos la tríada de principios de seguridad (Confidencialidad, Integridad, Disponibilidad) se observa que, en un entorno de TI, los esfuerzos se centran principalmente en garantizar la Confidencialidad de la información (como sería proteger la información personal, proteger las transacciones económicas, cifrar las comunicaciones, etc.) mientras que en un entorno de Tecnologías de la Operación (TO) la prioridad será garantizar la Disponibilidad, esto es, ofrecer el servicio de manera continua, evitando o minimizando los cortes o interrupciones, aumentando su ciber-resiliencia.

Por ello, también es de interés, como aquí se muestra, conocer cuáles han sido los principales incidentes de seguridad que han afectado al sector industrial, con especial relevancia en la región de América Latina y Caribe.

El informe viene acompañado por una herramienta de autoevaluación que le permitirá a cada empresa evaluar el estado de la ciberseguridad por medio del cálculo de un indicador de nivel de madurez basado en el marco ES-C2M2 (Electricity Subsector Cybersecurity Capability Madurity Model). Este instrumento se describe en el capítulo 4 *Recomendaciones a operadores del subsector eléctrico*, donde se comentan las acciones mínimas recomendadas para establecer una línea base de cumplimiento de requisitos relacionados con la ciberseguridad en la operación.

Finalmente, uno de los objetivos del estudio es proporcionar recomendaciones a los responsables de establecer políticas y estrategias de seguridad en los estados de la región, describiendo de manera general y específica los pasos básicos necesarios para establecer, apoyar y mantener la infraestructura de seguridad cibernética industrial que garantizará un nivel de seguridad eficiente y continuo en la protección de los sistemas industriales de las compañías del subsector eléctrico en ALC.

02 DEFINICIONES Y LISTAS DE ACRÓNIMOS

2.1 | Organizaciones

CIER
Comisión de Integración Energética Regional.

BID
Banco Interamericano de Desarrollo.

IEEE
Instituto de Ingenieros Eléctricos y Electrónicos.

IEC
International Electrotechnical Commission.
Comisión Electrotécnica Internacional

IIC
Industrial Internet Consortium
Consorcio industrial del Internet

ISA
International Society of Automation.
Sociedad Internacional de Automatización

ISO
International Standardization Organization.
Organización Internacional para la Estandarización

ALC
América Latina y el Caribe.

OEA
Organización de los Estados Americanos

NERC –
North American Electric Reliability Corporation
Corporación Norteamericana de Confiabilidad Eléctrica

NIST –
National Institute of Standards and Technology.
Instituto Nacional de Estándares y Tecnología Asociado al Departamento de Comercio de los Estados Unidos de América

ERM
Enterprise Risk Management
Gestión de Riesgos Empresariales

2.2 Normas, Estándares y Marcos de Referencia relacionados con Ciberseguridad Industrial en el Sector Energético

IEEE 1402

"Guía para la seguridad física y electrónica en subestaciones eléctricas".

Publicación del IEEE que trata aspectos de seguridad en subestaciones de suministro eléctrico. Incluye diferentes métodos y técnicas orientadas a prevenir la intrusión humana.

NERC CIP

"North American Electric Reliability Corporation Critical Infrastructure Protection".

Conjunto de estándares del NERC para la Protección de las Infraestructuras Críticas (CIP) orientado a proteger las redes de distribución de energía eléctrica frente a ciberataques o incidentes de seguridad que comprometan la disponibilidad del servicio energético en los Estados Unidos de América.

ES-C2M2

"Electricity Subsector Cybersecurity Capability Maturity Model".

El Modelo de Madurez de Capacidad en Ciberseguridad (C2M2) del Subsector Eléctrico (ES) es un modelo creado por el Departamento de Energía de los Estados Unidos de América para adaptar el modelo C2M2 en los procesos de evaluación y mejora de las capacidades de ciberseguridad en las compañías del subsector eléctrico.

ENISA Smart Grid Threat Landscape and Good Practice Guide

La publicación de ENISA describe que las redes eléctricas inteligentes son sistemas críticos complejos que almacenan, transportan y gestionan energía. Este desarrolla los principios como: considerar las amenazas externas e internas, descomponer y clasificar los elementos, y capturar el conocimiento disponible. De esta manera, el documento se convierte en una herramienta para la evaluación del riesgo de exposición de los activos y mostrar que se debe hacer al respecto.

ENISA Appropriate security measures for smart grids

La publicación de ENISA es un documento técnico que provee los lineamientos para las partes interesadas en redes eléctricas inteligentes. Estos son presentados como un conjunto de medidas de seguridad mínimas orientadas en apoyar la mejora de los niveles mínimos de los servicios de ciberseguridad. Las medidas se organizan en tres niveles de sofisticación y 10 dominios.

ENISA Communication network interdependencies in smart grids

Este estudio de ENISA se centra en la evaluación de las interdependencias y las comunicaciones entre todos los activos que conforman las nuevas redes de energía, sus arquitecturas y conexiones para determinar su importancia, amenazas, riesgos, factores de mitigación y posibles medidas de seguridad para implementar. Para obtener esta información, se contactó a expertos en los campos y áreas relacionadas directamente con las redes inteligentes para recopilar sus conocimientos y experiencia.

ENISA Smart Grid Security Certification in Europe

El informe de ENISA describe la necesidad de prácticas armonizadas de certificación de redes eléctricas inteligentes europeas que cubran toda la cadena de suministro de redes eléctricas inteligentes, y están respaldadas por una plataforma europea basada en M / 490 SGAM1 (Modelo de arquitectura de redes inteligentes) y el concepto de cadena de confianza de redes eléctricas inteligentes.

CEER Cybersecurity Report on Europe's Electricity and Gas Sectors

Este informe del Council of European Energy Regulators (CEER) describe la visión del panorama de ciberseguridad de las Autoridades Reguladoras Nacionales (NRA). El informe ofrece una descripción general del estado de la ciberseguridad en el sector energético, con un enfoque particular en la necesidad de confianza, el uso de la computación en la nube, el análisis de Big Data y el entorno legislativo europeo, incluida la Directiva NIS, GDPR y Clean Energy.

ISO/IEC 27019:2017

Establece guías de aplicación de los controles de la norma ISO/IEC 27002 en un sistema de gestión de la seguridad aplicado a los sistemas de control y automatización del sector energético. Tiene en cuenta las características propias del subsector eléctrico considerando su repercusión en el entorno de las infraestructuras críticas.

2.3 Normas, Estándares y Marcos de Referencia relacionados con Ciberseguridad Industrial

ISA/IEC 62443

Conjunto de estándares derivados de la norma ISA99 que comprende informes técnicos, especificaciones técnicas y guías agrupados en 4 bloques (General, Políticas y procedimientos, Sistema y Componentes) para ayudar en la protección de los Sistemas de Automatización y Control Industrial frente a incidentes de seguridad.

NIST SP 800-82

"Guía para la Seguridad de los Sistemas de Control Industrial (ICS)".

Publicación especial del NIST que provee una guía sobre cómo securizar los Sistemas de Automatización y Control Industrial, incluyendo sistemas SCADA, DCS y PLC, considerando las características de topología, amenazas y vulnerabilidades propias de los entornos industriales.

IC-IISF

"Industrial Internet Consortium (IIC) Industrial Internet Security Framework" (IISF)".

Marco de trabajo para evaluar y tratar los riesgos de seguridad en los entornos industriales, poniendo especial foco en los nuevos paradigmas como IIoT (Industrial Internet of Things), Smart Grids o Smart Metering.

2.4 Normas, Estándares y Marcos de Referencia relacionados con Ciberseguridad

Common Regulatory Framework on Cybersecurity (CRF)

Iniciativa sectorial en el marco de la UNECE (United Nations Economic Commission for Europe) para promover la convergencia de las regulaciones técnicas nacionales hacia un marco compartido con un enfoque basado en el riesgo y otras mejores prácticas reconocidas internacionalmente, con el espíritu de reducir las barreras para la comercialización de componentes, equipos, personas y servicios cualificados y aumentar la confiabilidad, continuidad, seguridad y protección de los servicios esenciales.

ISO/IEC 27001

Estándar internacional para Sistemas de Gestión de la Seguridad de la Información. - Este estándar especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el Ciclo de Deming o Ciclo PDCA (acrónimo de Plan, Do, Check, Act).

ISO/IEC 27002

Estándar internacional que proporciona un código de buenas prácticas para los responsables de iniciar, implantar o mantener un SGSI. Para este fin, incluye un conjunto de 114 objetivos de control y gestión que deberían ser perseguidos por las organizaciones.

NIST SP 800-39

"Gestión de riesgos de seguridad de la información"

El propósito de la Publicación especial 800-39 es proporcionar una guía para un programa

integrado de toda la organización para administrar el riesgo de seguridad de la información para las operaciones de la organización (es decir, misión, funciones, imagen y reputación), activos e individuos. La Publicación especial 800-39 proporciona un enfoque estructurado, pero flexible para administrar el riesgo de seguridad de la información que tiene una base intencionalmente amplia, con los detalles específicos de evaluación, respuesta y monitoreo del riesgo de forma continua proporcionados por otros estándares y pautas de seguridad de NIST de respaldo.

La guía proporcionada en esta publicación no pretende reemplazar o subsumir otras actividades, programas, procesos o enfoques relacionados con el riesgo que las organizaciones han implementado o tienen la intención de implementar para abordar las áreas de gestión de riesgos cubiertas por otras leyes, directivas, políticas, iniciativas programáticas, o misión / requisitos del negocio. Más bien, la guía de gestión de riesgos de seguridad de la información que se describe en este documento es complementaria y se puede utilizar como parte de un programa de gestión de riesgos empresariales (ERM) más completo [1].

NIST SP 800-53

"Controles de seguridad y privacidad para organizaciones y sistemas de información".

Publicación especial del NIST que provee un conjunto de controles para la protección frente a diversas amenazas, incluyendo ataques hostiles, desastres naturales, fallos estructurales, errores humanos y riesgos de privacidad.

2.5 Términos relacionados con sistemas de control industrial

TO
"Tecnologías de la Operación"
Conjunto de equipos, sistemas y redes que componen los sistemas de automatización y de control en entornos industriales. Intervienen en la operación de los procesos de producción.

ICS
"Sistemas de Control Industrial"
Sistemas utilizados para el control, monitorización y supervisión de los procesos industriales. Están conectados a los elementos que intervienen en el proceso (sensores y actuadores) y pueden interactuar con ellos enviando órdenes o recibiendo datos.

IACS
"Sistemas de Automatización y Control Industrial"
Término equivalente a ICS.

IoT
"Internet of Things (Internet de las cosas)".
Cualquier dispositivo o elemento electrónico con capacidades de computación y comunicación capaz de transferir datos a través de la red sin necesidad de intervención humana ni de un computador.

IIoT
"Industrial Internet of Things"
Designa a los elementos IoT diseñados para operar específicamente en entornos industriales.

Modelo Purdue
Modelo de arquitectura de referencia adoptado por la ISA para clasificar los elementos de un sistema industrial en un modelo de 5 capas (Algunas veces se considera una capa adicional relacionada con la alta dirección). De utilidad en la implantación de medidas de seguridad ya que permite segmentar una instalación industrial según la red correspondiente a cada capa del modelo.

Proceso operativo
El proceso operativo (o proceso industrial) es una colección de procedimientos de automatización realizados por el sistema para lograr el producto o servicio final a tiempo, con precisión y seguridad, manteniendo la calidad deseada del producto. El proceso operativo está controlado y automatizado por los elementos IACS.

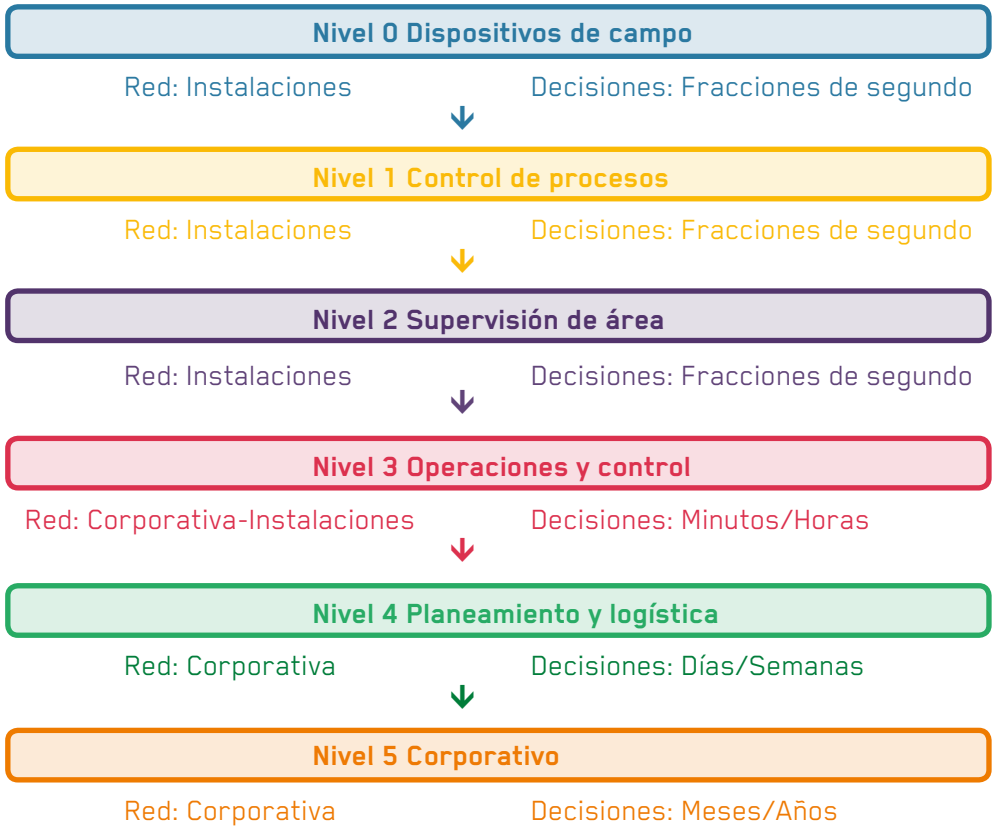


FIGURA 1. Modelo de Purdue tomado de [2]

Protocolo de comunicación industrial

Protocolo utilizado en una red de control para la comunicación de los distintos dispositivos de campo o de control (sensores, actuadores, PLC, DCS, etc.).

Los buses de campo pueden utilizar conexiones y protocolos específicos como Profibus, Profinet o FieldBus, a través de distinta tipología de redes físicas, incluyendo comunicaciones serie RS-232/485.
Los elementos de control utilizan protocolos propietarios del fabricante u otros de carácter general como Modbus, DNP3 o OPC-UA.

Smart Grid

Red de distribución de energía eléctrica que incorpora capacidades de comunicación digital bidireccional entre la instalación (proveedor) y el usuario. Permite monitorizar y medir el comportamiento eléctrico de la infraestructura.

Smart Meter

Contador Inteligente o Telecontador
Sistema de medición electrónica inteligente que permite medir el consumo en tiempo real y la interacción entre el consumidor y la compañía suministradora (tarificación personalizada, monitorización remota, corte del suministro, etc.). De aplicación en cualquier tipo de suministro (energía eléctrica, agua, gas...).

2.6 | Elementos de un Sistema de Control Industrial

Dispositivos de Campo (Sensores y Actuadores)

Dispositivos electromecánicos que interactúan directamente en el proceso industrial, ya sea capturando datos del proceso (sensores de temperatura, contadores de paso, medidores de tensión, medidores de nivel, etc.) o generando acciones (relés, válvulas electromecánicas, variadores, servos, etc.). Se conectan a un elemento de control mediante un bus de campo.

CPS

Sistemas Ciber-Físicos

Dispositivos de Campo que incorporan capacidades avanzadas de computación y comunicación, pudiendo conectar directamente con los elementos de control a través de redes de comunicación estándar (incluso Wi-Fi o Internet) sin necesidad de buses de campo.

PLC

Controlador

Lógico Programable

Dispositivo con la capacidad de trasladar una señal lógica (bits) en una respuesta física sobre un elemento TO y actuar sobre el proceso (por ejemplo, abrir o cerrar una válvula, variar la velocidad de un motor). Se trata de un elemento programable, de modo que un mismo dispositivo puede realizar funciones diversas según la finalidad para la que haya sido programado.

DCS

Sistemas de Control Distribuido

Sistema de control compuesto por diferentes equipos interconectados entre sí que forman parte de un mismo proceso. Tienen la capacidad de intercambiar entre ellos datos para el control y supervisión del proceso principal.

RTU

Unidad Terminal Remota

Dispositivos OT para la recepción o envío de señales de control en ubicaciones alejadas del sistema de control principal.

SCADA

Control de Supervisión y Adquisición de Datos

Sistema de control que utiliza ordenadores, comunicaciones de datos en red e interfaces gráficas de usuario para la gestión de supervisión de procesos de alto nivel. Recopila la información de los elementos de control (PLC, DCS) y permite tener una visión global de todo el proceso industrial. Tiene capacidades de análisis de los datos y puede enviar instrucciones a los controladores programables para interactuar con el proceso.

HMI

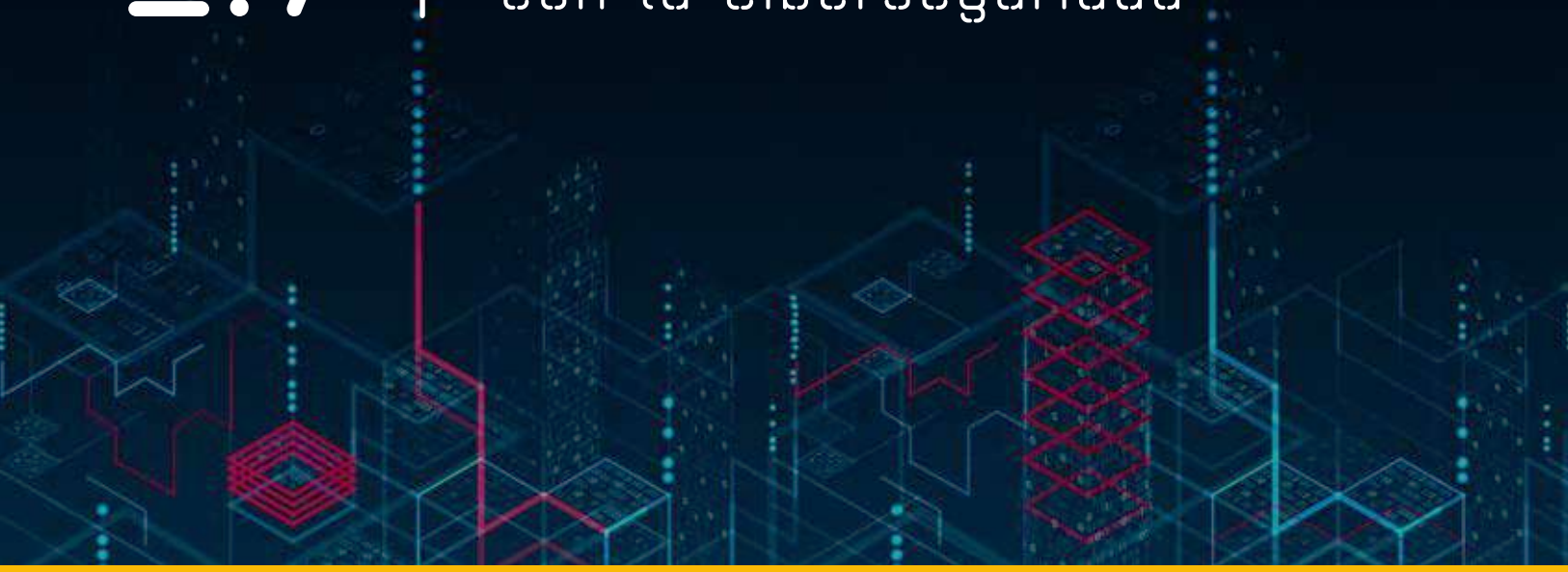
Interfaz Hombre-Máquina

Dispositivo con interfaz de usuario mediante el cual un operador puede visualizar y actuar sobre el estado del proceso o detectar alertas. Algunos HMI tienen una pantalla táctil o botones de función que permiten al operario interactuar con el proceso, en especial cuando hay alarmas que atender.

Estación de Ingeniería (ENG)

Equipo que permite la conexión a uno o varios dispositivos, generalmente a un PLC, para actuar sobre su lógica. Permite configurar sus parámetros, actualizar su firmware, programarlo, cargar/descargar programas y configuraciones o realizar cualquier otra acción sobre la lógica del PLC que el fabricante permita.

2.7 | Términos relacionados con la Ciberseguridad



Activo
Cualquier elemento que forme parte de un servicio o proceso de operación que deba ser protegido para garantizar la continuidad y calidad del servicio.

Amenaza
Cualquier acción o elemento, ya sea interno o externo, capaz de causar daño a un activo.

Vulnerabilidad
Debilidad en un activo o en el proceso del cual forma parte que podría exponer el sistema a la materialización de una amenaza.

Riesgo
Combinación de la probabilidad de que una amenaza impacte sobre un activo y de sus consecuencias. El riesgo se mitiga a través de la implantación de controles de seguridad.

Superficie de ataque
Conjunto de vulnerabilidades que permitirían acceder a un sistema por parte de un atacante. La superficie de ataque se utiliza para obtener acceso no autorizado, interrumpir las comunicaciones y el acceso a datos, y degradar el servicio o producto generado por el sistema.

Vector de ataque
Método que el atacante utiliza para acceder a un sistema, a través del cual podrá introducir los códigos maliciosos o herramientas para infectar un sistema.

Firewall
Dispositivo de seguridad perimetral que permite administrar y controlar el tráfico y los servicios de red. Suele instalarse en puntos de entrada/salida o interconexión de redes para poder analizar todo el tráfico que circula por ese punto.

IDS
Sistema de detección de intrusiones. Supervisa los datos/tráfico y genera alarmas.

IPS
Sistema de prevención de intrusiones. Supervisa los datos/tráfico, genera alarmas y bloquea activamente el tráfico para mitigar el ataque.

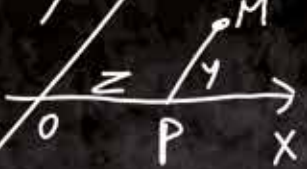
Diodo de datos
Dispositivo que permite que el tráfico de red se mueva sólo en una dirección. El principio de funcionamiento se basa en el aislamiento físico de la comunicación. Utilizado como medida de seguridad en entornos muy críticos como centrales nucleares.

SIEM
Sistema de gestión de información y eventos de seguridad. Elemento de seguridad de red que recopila información (logs) de seguridad de los equipos de la red y permite correlar los eventos y analizarlos de forma conjunta.

SOC
Centro de Operaciones de Seguridad. Instalación donde se realiza el seguimiento y análisis de la actividad de red de una compañía desde el punto de vista de seguridad. Un equipo de especialistas supervisa y gestiona los equipos (servidores, routers, firewalls, redes...) para detectar y responder ante cualquier incidente de seguridad.

CSIRT
Equipo de Respuesta frente Incidentes de Seguridad. Equipo de especialistas en seguridad que actúan cuando se produce un incidente para restablecer el servicio o proceso al estado previo a la incidencia. En ocasiones pueden disponer también de capacidades de prevención (operando junto con el SOC) o de análisis post-incidente (DFIR: *Digital Forensics and Incident Response*).

CISO
Director de Seguridad de la Información.



$d = \sqrt{(8,5+2,3)^2 + (0,7-4)^2} =$

$\sqrt{10,8^2 + 3,3^2} \approx 11,3$

$x = \frac{18}{5} = 3.6 \quad y = -\frac{12}{5} = -2,4$

$= m_1 : m_2 = -2$

$m_1 = -2, \; m_2 = 1 \qquad m_1 = 2, \; m_2 = -1$

$= 49$

$x = \frac{1 \cdot 1 + (-2) \cdot 3}{-2+1} = 5$

$\approx 6,22$

$y = \frac{1 \cdot 2 + (-2) \cdot 3}{-2+1} = 4$

$= -3,22 \quad x = \frac{x_1 + x_2}{2}, \; y = \frac{y_1 + y_2}{2}$

$m_1 = m_2 = 1 \qquad \lambda = 1$

$= -3,22$

(L)

$6,22$

$x + y = 3$

$^2 + y^2 = 4$

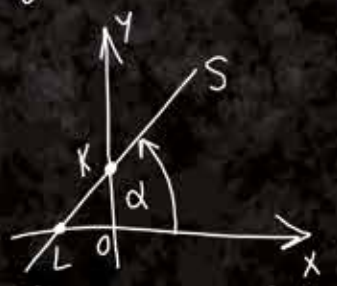
$x = \frac{x_1 + \lambda x_2}{1+\lambda}, \; y = \frac{y_1 + \lambda y_2}{1+\lambda}$

$m_1 = 2, \; m_2 = 3, \; x_1 = 6, \; y_1 = -4, \; x_2 =$

$y = ax + b$

$a = tg\, \alpha = tg \angle xLS$

$a = tg(-45^\circ) = -1 \qquad y = -x - 3$



$f > 0 \qquad f < 0 \qquad x = 0 \qquad b = 3$

$y = 3$

$\underline{b} = \frac{1}{2}(\underline{a} + \underline{c})$

$Ax + By + C = 0$

$y = b$

$b > 0$

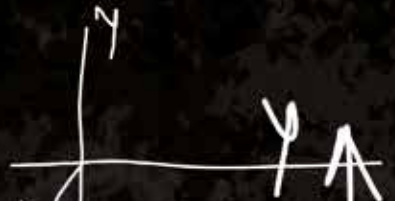
$b < 0, \; y = 0$

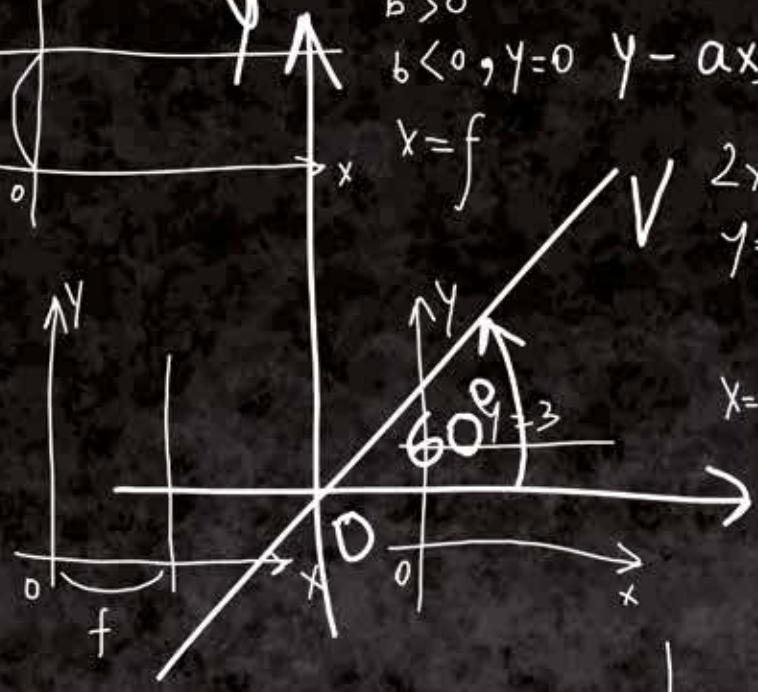
$y - ax + b \left(a = -\frac{A}{B}, \; b = -\frac{C}{B} \right)$

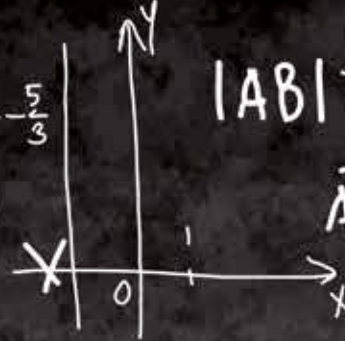
$x = f$

$2x - 4y + 5 = 0 \; (A = 2, B = -4, C = 5)$

$y = 0,5x + 1,25 \; \left(a = -\frac{2}{-4} = 0,5, \; b = \right.$







$|AB| : |BC| = \lambda :$

$\overrightarrow{AC} = (c - a),$

$= b - a$

$A_1(x_1, y_1) \quad b = 1$

$A_2(x_2, y_2)$

$A_1K : KA_2 = m_1 : m_2$

$A_1(x_1; y_1) \quad A_2(x_2; y_2)$

$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$

2.8 | Tipos de ciberataques

Ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS)

Ataque lanzado desde un gran número de máquinas ejecutando solicitudes hacia el sistema víctima de modo que éste queda saturado y pierde la capacidad de respuesta.

Ataques de *phishing* y *spear phishing*

Ataque vía correo electrónico que confunde a la víctima para descargar o permitir el acceso a contenido malicioso. Puede ser una campaña genérica o un ataque adaptado a individuos concretos o grupos específicos combinando técnicas de ingeniería social (*spear phishing*).

Ataque de Hombre en el medio (*Man-in-the-Middle*)

Ataque que consigue redirigir el tráfico en la red host para pasar a través de la red del atacante, lo que le permite capturar o manipular los datos del tráfico.

APT

Amenazas Persistentes y Avanzadas – ataque sofisticado sobre un objetivo concreto y definido con el fin de obtener un beneficio de ello. Las APT requieren mucha investigación previa sobre la víctima y suelen requerir mucho tiempo de preparación y equipos de cibercriminales altamente especializados.

Ataque de fuerza bruta

Ataque que trata de descubrir la contraseña de las víctimas con herramientas automatizadas que generan todas las combinaciones posibles de claves hasta encontrar la correcta.

Ataque de inyección SQL

Ataque que aprovecha una falta de validación en la entrada (*input*) de comandos a una base de datos SQL mediante la introducción de cadenas y caracteres específicos para entregar datos no autorizados de la base de datos.

Cross-site scripting (XSS)

Ataques que aprovechan vulnerabilidades en un sitio web para inyectar secuencias de comandos (*scripts*) no autorizados que engañan al usuario para obtener datos privados mediante la transferencia, sin conocimiento de la víctima, a un sitio falso que se asemeja al original.

Malware

Cualquier tipo de código malicioso diseñado para obtener acceso a los sistemas y a la red de la víctima y llevar a cabo diferentes tipos de ataques. Entre los códigos maliciosos más comunes podemos citar a los virus, gusanos, troyanos, *rookits*, *keyloggers*, *ransomware*, etc.

03

EVALUACIÓN CUALITATIVA, CUANTITATIVA Y ENTENDIMIENTO DEL ESTADO DEL ARTE

A diferencia de otro tipo de sistemas interconectados, como es el caso del *world wide web* (WWW) donde la caída de un nodo no supone la caída del sistema, la red de interconexión eléctrica sí es susceptible a este tipo de amenaza. En una red de transmisión de energía, cada nodo (estación de energía) debe gestionar la carga de potencia. La remoción de nodos sea por apagones aleatorios o ataques intencionados, cambia el balance del flujo y lleva a una redistribución global de las cargas en todas las redes. Esto puede generar una cascada de apagones debido a la sobrecarga. [3]

Es a partir de este entendimiento de la complejidad de la operación que se plantea cómo esta infraestructura crítica es susceptible a múltiples amenazas que pueden afectar la disponibilidad del servicio.

3.1 | Estado del arte en incidentes de seguridad

Kaspersky Lab[1] comisionó un estudio del estado de la ciberseguridad industrial [4] a nivel global mostrando algunos resultados relevantes. Para la región de ALC y África se muestra que un 68% de las empresas consideran probable ser víctimas de un ciberataque a su infraestructura TO.

1. Kaspersky Lab es una compañía multinacional de ciberseguridad y proveedor comercial de software antivirus.

Se establece en el estudio el siguiente listado de los cinco mayores incidentes que generan preocupaciones:

- **Ataques dirigidos y APT**
- **Malware convencional y nuevos virus**
- **Ataques de Ramsomware**
- **Filtración de datos y espionaje**
- **Sabotaje u otro daño físico intencional causado por actores externos**

También se indica que al menos un 31% de los participantes fueron víctimas de uno de estos incidentes en el último año.

También se indica que al menos un **31%** **de los participantes fueron víctimas** de uno de estos **incidentes** en el último año. [4]

En contraste, las cinco mayores causas de incidentes según el estudio se corresponden con:

- **Malware convencional y nuevos virus**
- **Ataques de ramsomware**
- **Errores de los empleados y acciones no intencionales**
- **Amenazas por otros actores como la cadena de suministro o proveedores**
- **Fallas en el hardware**

Las **consecuencias** de estas **acciones** se reflejan en:

- **Daños en la calidad de los productos o servicios**
- **Pérdida de la confianza de los clientes**
- **Daño al ambiente**
- **Pérdida de contratos u oportunidades de negocio**
- **Daño al equipo**

Kaspersky [4] muestra en el estudio la alta tendencia que hay para moverse a soluciones de IoT (Smart Energy) y soluciones de SCADA en la nube. Esto va de la mano con un aumento en la inversión en los dos siguientes años y que la amenaza de que se materialicen los riesgos o se repitan los incidentes son los mayores criterios para la definición de un presupuesto.

La producción de energía limpia es una preocupación en la Unión Europea donde se han generado múltiples paquetes que estimulan y regulan su producción. Estos intentan tocar aspectos no solucionados aún y relacionados con la ciberseguridad. De manera particular, los planes de preparación de riesgos deben ser consistentes y actualizados tanto a nivel nacional como regional, buscando ser efectivos en escenarios de ciberseguridad. [5]

En la actualidad, las soluciones basadas en la nube son cada vez más comunes y ofrecen una versatilidad que hoy la TI asume como natural. Las empresas del sector de la energía aún no tienen claro cuan seguro es ir a la nube, sobre todo en factores de riesgo como ciberdelincuentes, ramsomware, ciberataques que faciliten la realización de apagones, debilidades de la seguridad de los datos y filtración de la información y eventos que puedan afectar la privacidad de la información operativa y que estén sujetos al marco del Reglamento General de Protección de Datos de la Unión Europea (GDPR) [5].

Actualmente los sistemas **SCADA/ ICS** son usados en **funciones** como:

Generación

Transmisión

Distribución

Cuando la tecnología SCADA nació el internet no existía, por ello brindar seguridad a redes SCADA para ataques basados en internet o la infiltración de la cadena de suministro global no fueron consideraciones iniciales cuando se diseñó la red de soporte de esta infraestructura crítica. [6]

De acuerdo con el reporte de la Oficina del Director de Inteligencia Nacional de los Estados Unidos [6] las amenazas a la malla eléctrica son múltiples y variadas. Nuevas tecnologías crean nuevas vulnerabilidades y los adversarios desarrollan nuevo malware y todo tipo de métodos para explotarlas.

El informe indica que hay pocos incentivos para invertir en medidas que mitiguen las vulnerabilidades asociadas con las nuevas tecnologías. Esto incrementa la probabilidad y la efectividad de los ataques cibernéticos a las tecnologías operacionales en la red eléctrica.

Actualmente, los sistemas TI y TO están más integrados (ver Figura 2), son más complejos y presentan vulnerabilidades. Cuando las instalaciones de generación y distribución transfieren el control de sus equipos desde sus infraestructuras internas a sistemas SCADA, los cuales tienen acceso a través de internet, están introduciendo ciber vulnerabilidades. [6]

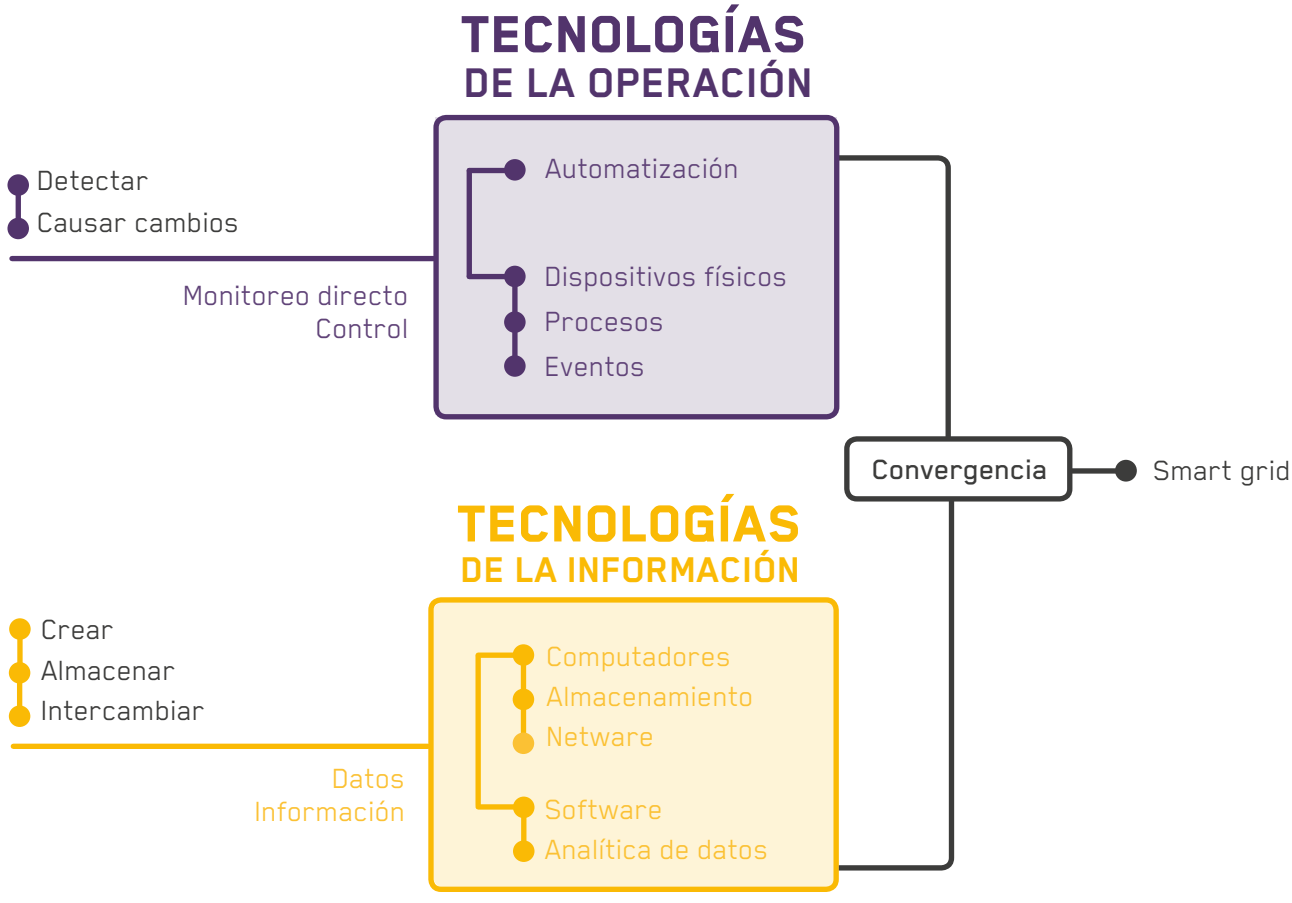


FIGURA 2. Convergencia TI y TO.

El Centro de Ciberseguridad Industrial (CCI) [7] establece dos definiciones importantes a considerar:

"El término Infraestructura Crítica es empleado por los Estados para definir instalaciones y sistemas sobre los que recaen servicios esenciales cuyo funcionamiento no permite soluciones alternativas." [7]

"La Ciberseguridad Industrial aborda la prevención, monitorización y mejora de la resistencia de los sistemas industriales y su recuperación, ante acciones hostiles o inesperadas que puedan afectar al correcto funcionamiento de los procesos industriales." [7]

Un aspecto para resaltar es que "tanto la Ciberseguridad Industrial, como la Protección de Infraestructuras Críticas requieren la realización de evaluaciones de riesgos con el fin de determinar sobre qué componente actuar y qué medidas deben ser adoptadas para disminuir el riesgo afrontado" [7]. Esto quiere decir que el proceso de toma de decisión debe estar basado en datos y en riesgos, para que le permita tanto a los legisladores como a los responsables de seguridad responder de manera eficaz y eficiente a sus necesidades.

El documento del CCI [7] hace un recorrido por diferentes marcos de buenas prácticas y regulaciones relacionadas con la ciberseguridad industrial y de infraestructuras críticas, mostrando que para Latinoamérica aún falta mucho por hacer, y que se está avanzando de manera individual en cada país.

Mucha de la literatura hoy resalta el evento de Stuxnet en 2010 como uno de los más relevantes o el ataque a la red eléctrica de Ucrania (BlackEnergy en 2015 e Industroyer en 2016), pero para el interés de este estudio, hay varios eventos antes y

CRONOLOGÍA

FIGURA 3. Línea de tiempo de incidentes de ciberseguridad industrial 1980-2003

FIGURA 4. Línea de tiempo de incidentes de ciberseguridad industrial 2003-2012

FIGURA 5. Línea de tiempo de incidentes de ciberseguridad industrial 2014-2017

FIGURA 6. Línea de tiempo de incidentes de ciberseguridad industrial 2017-2018

FUENTE. Basado en CRITIFENCE 2018 Critical Infrastructure Cyber Attack Timeline www.critifence.com

después que revelan cómo han evolucionado los incidentes.

Se presenta una breve cronología de incidentes de ciberseguridad que afectan infraestructuras críticas, y de manera especial al sector de energía.

Un aspecto para resaltar son los ataques que tienen como objetivo los sistemas de control industrial. Por ejemplo, la campaña de ataque Havex de 2014 por medio de una familia de malware que tenía la habilidad de encontrar otros ICS. [8]

Las campañas Sandworm en 2014 explotaron una vulnerabilidad de los equipos HMI de GE. Este sirvió de preámbulo para los ataques de Ucrania (en 2015 y 2016) y en Estados Unidos en 2016, según un estudio de Trend Micro. [8]

Ataques como los generados por el equipo TRITON revelaron la necesidad que los sistemas de seguridad y protección (Safe and Security) deban estar en redes aisladas [9], ya que pueden ser vulnerables a ataques y poner en riesgo vidas humanas. Desde el 2016 hasta el 2018 se han registrado ataques que implican también espionaje a empresas del sector eléctrico tanto en Estados Unidos como en Turquía o Irlanda. [8]

El estudio de Trend Micro también revela que un vector de ataque es ofrecido por las mismas empresas al colocar sus sistemas (HMI, SCADA, entre otros) en internet, es decir con IP públicas, y expuestos sin ninguna medida de seguridad más que un usuario y una contraseña, que en algunos casos es la genérica definida por el fabricante. Estos sistemas son fácilmente descubiertos por plataformas como SHODAN y técnicas como GeoStalking. [8]

INCIDENTES DE **CIBERSEGURIDAD** INDUSTRIAL

1982
Farewell Dossier
Estados Unidos
Troyano

1992
Sistema de Alerta de Emergencias
Chevron, Estados Unidos
Mal uso de recursos

1994
Proyecto Salt River
Estados Unidos
Troyano

1997
Aeropuerto Worcester
Massachusetts, Estados Unidos
Compromiso root, DoS

1999
Operación Gazprom
Rusia
Troyano

1999
Gasoducto Bellingham
Washington, Estados Unidos
Mal uso de recursos

2000
Acueducto Maroochy
Australia
Mal uso de recursos

2001
Operador del Sistema Eléctrico (CAISO)
California, Estados Unidos
Compromiso root

2002
Puerto Marítimo
Venezuela
Consola remota

2003
Slammer
Planta nuclear David - Besse,
Estados Unidos
Virus

1980-2003

FIGURA 3. Línea de tiempo de incidentes de ciberseguridad industrial 1980-2003 [10], [11].

2003-2012

2003
Israel Electric Corp. (IEC)
Israel Electric Corp, Israel
DoS

2003
Sobig
CSX Corporation, Estados Unidos
Virus

2004
Sasser
British Airways Railcorp,
Delta, Reino Unido
Virus

2005
Zotob
Daimler Chrisler AG, Estados Unidos
IRCBot

2007
Tehama Colusa (TCAA)
Autoridad del canal, Estados Unidos
Mal uso de recursos

2009
Conficker
Armada francesa, Francia
Worm

2010
Stuxnet (Dugu, Flame y Gauss)
Planta nuclear Natanz, Irán
Worm

2011
Operación Night Dragon
Exxon, Shell, BP, Estados Unidos
Troyano de acción remota (RAT)

2011
DUQU
Hemisferio Occidental,
Medio Oriente, Asia
Malware, virus

2012
Flame
Ministerio del Petróleo,
Compañía Nacional de Petróleo, Irán
Malware, worm

FIGURA 4. Línea de tiempo de incidentes de ciberseguridad industrial 2003-2012 [10], [11].

INCIDENTES DE **CIBERSEGURIDAD** INDUSTRIAL

2014
Havex
Múltiples objetivos
(no revelados)
Botnet, troyano

2014
Troyano Siemens
Escala mundial (desconocida)
Actualización de software

2015
Onion City
Corea del Sur
Botnet, troyano

2015
BlackEnergy
Red eléctrica, Ucrania
Malware, spear phishing

2016
Conflicker
Planta nuclear KGG, Alemania
Worm

2014-2017

2014
Blacken
General Electric (GE), Estados Unidos
Botnet, troyano

2014
OnionDog
Corea del Sur
Malware, USB worm

2015
Fábrica de Acero
Alemania
Malware, spear phishing

2016
Grupo de hackers sirios
Compañía de agua Kemuri (KWC),
Spear phishing

2017
Crashoverride
Red eléctrica, Ucrania
Worm

FIGURA 5. Línea de tiempo de incidentes de ciberseguridad industrial 2014-2017 [10], [11].

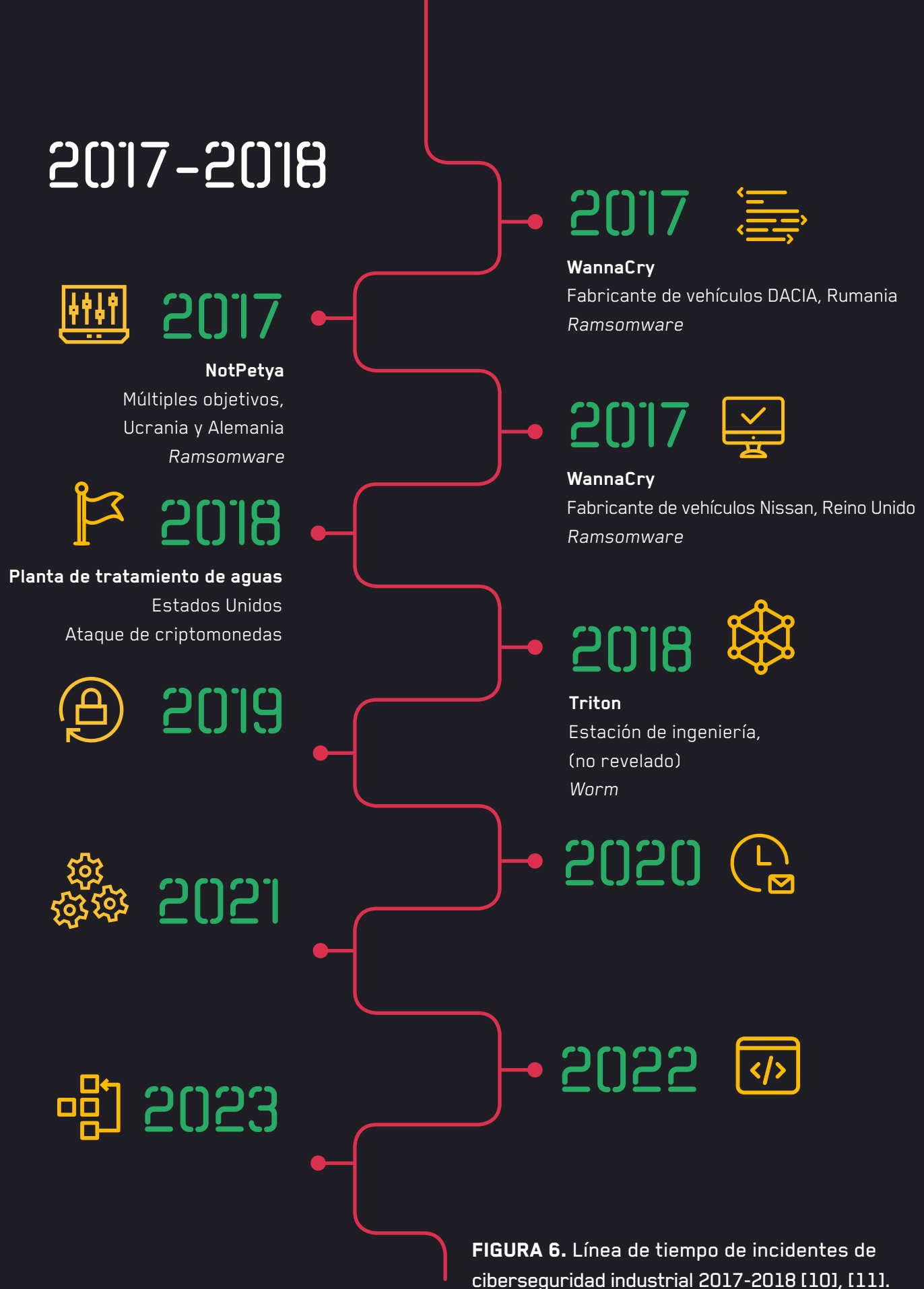


FIGURA 6. Línea de tiempo de incidentes de ciberseguridad industrial 2017-2018 [10], [11].

Algunas **lecciones aprendidas** a partir de los ataques a tecnologías **SCADA/ICS [6]:**

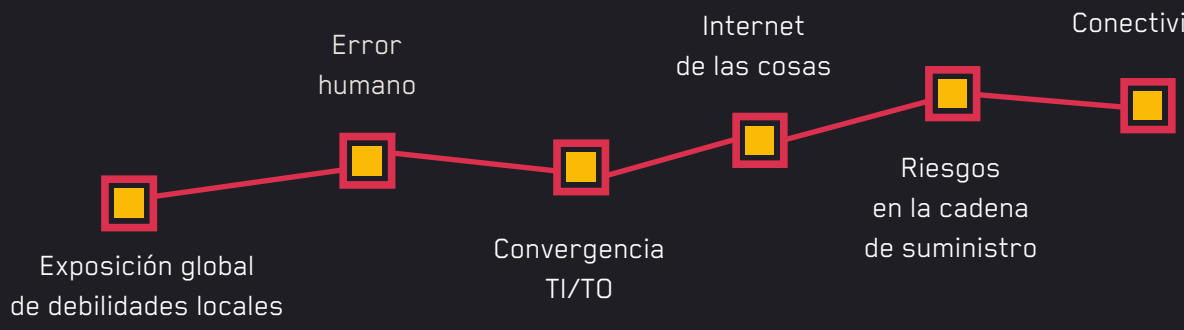


FIGURA 7. Algunas lecciones aprendidas.

3.2 | Estado del arte en tecnologías de protección

En [6] se enuncian algunos factores de riesgo en sistemas SCADA e ICS para la red eléctrica, como:

1. Convergencia entre TI y TO

2. Los usuarios optimizan el sector eléctrico con sistemas SCADA.

3. El incremento de vulnerabilidades operacionales y cibernéticas como resultado del uso de SCADA e ICS.

4. La llegada de nuevos participantes y la globalización hace que la cadena de suministro sea un claro vector de ataque para SCADA e ICS.

5. El incremento de la frecuencia de los ataques que apuntan a instalaciones alrededor del mundo.

Entendiendo al
riesgo como:

Riesgo=f (Probalidad (amenaza, vulnerabilidad), Impacto (consecuencias, integridad, disponibilidad))

Las opciones de mitigación buscan:

- → Reducir la probabilidad de que la amenaza se materialice explotando la vulnerabilidad o
- → Reducir las consecuencias del riesgo en la confidencialidad o integridad de los datos (infraestructura TI) y señales (infraestructura TO), así como en la disponibilidad de los sistemas industriales y TIC.

Algunas estrategias de mitigación pueden incluir un enfoque como en la Figura 8.

TECNOLOGÍAS

- Uso de información y BIG DATA para ejecutar pruebas, medición y detección de potenciales intrusiones.
- Las redes deben ser segmentadas, monitoreadas y controladas.
- Limitar el acceso al ICS y a la información de la red de control que existe sobre la red de negocio.
- La implementación de múltiples factores de autenticación.
- Incluir VPN dentro del ICS que vengan de la red de negocios.

POLÍTICAS Y REGULACIONES

- Guías y estándares de la industria e incentivos.
- Regulaciones que incluyan requerimientos legales, auditorías y sanciones relacionadas con el establecimiento de requerimientos de seguridad.

PROCESOS

- Compartir información.
- Desarrollar medidas activas para la gestión del riesgo en la cadena de suministro.
- Ciberdefensas.
- Planes de respuesta a incidentes que incorporen personal tanto de TI como de TO.
- Planes de operación resilientes para sobrevivir a ataques cibernéticos, a la TO y la sostenibilidad del sistema.

FIGURA 8. Enfoques de mitigación del riesgo.

3.3 | Definición de las organizaciones entrevistadas

Se considera un modelo de red eléctrica en el cual la cadena de suministro está basada en la generación de energía eléctrica y su transmisión hasta el cliente final. Se consideran los generadores de energía, proveedores de energía (incluidos los comercializadores, comerciantes y corredores de energía), proveedores de servicios de transmisión y consumidores (mercados de demanda, usuarios finales). [12]

Los generadores de energía son aquellos que toman las decisiones relacionadas con la posesión y operación de las instalaciones de generación eléctrica o plantas de energía. Producen energía eléctrica, que luego se vende a los proveedores de energía. Los proveedores de energía, en cambio, tienen la función de intermediario. Compran energía eléctrica de generadores de energía y la venden a los consumidores en diferentes mercados de demanda. [12]

Para que la electricidad se transmita desde un generador de energía hasta el punto de consumo, se requiere un servicio de transmisión. Por lo tanto, los proveedores de energía deben comprar los servicios de transmisión de los proveedores de servicios de transmisión. Los proveedores de servicios de transmisión son aquellas entidades que poseen y operan los sistemas de transmisión y distribución eléctrica. Estas son las empresas que distribuyen electricidad de los generadores a través de proveedores a los mercados de demanda (hogares y empresas). [12]

El último tipo de tomador de decisiones en el modelo son los consumidores o los mercados de demanda. Estos son los puntos de consumo de energía eléctrica. Los consumidores generan la demanda que impulsa la generación y el suministro de energía eléctrica en todo el sistema. [12]

3.3.1 | Por segmento de actividad

PREGUNTAS ORIENTADORAS

¿Qué **sector industrial** describe mejor **el modelo de negocio** de su empresa?

Se realizó una convocatoria a todas aquellas empresas que hacen parte de la cadena de suministro, identificándose el segmento al que pertenecían:

Generación

Transmisión

Distribución

Operación del sistema

También se permitió que se identificaran como organizaciones multisegmento.

La muestra está compuesta por 43 organizaciones clasificadas de acuerdo con la Figura 9, donde se presenta la participación por segmento. Esta clasificación es utilizada en el estudio como base para el análisis.

Una de las limitaciones del estudio radica en el hecho que no todas las organizaciones participantes respondieron a la totalidad de las preguntas. Este aspecto es muy relevante, puesto que limita el análisis de muchas de las preguntas a resolver. Por ello, se considera relevante reflejar cuántas organizaciones no respondieron a las preguntas, con el ánimo de estimular para futuros ejercicios un compromiso mayor para lograr un reflejo más fiable del escenario.

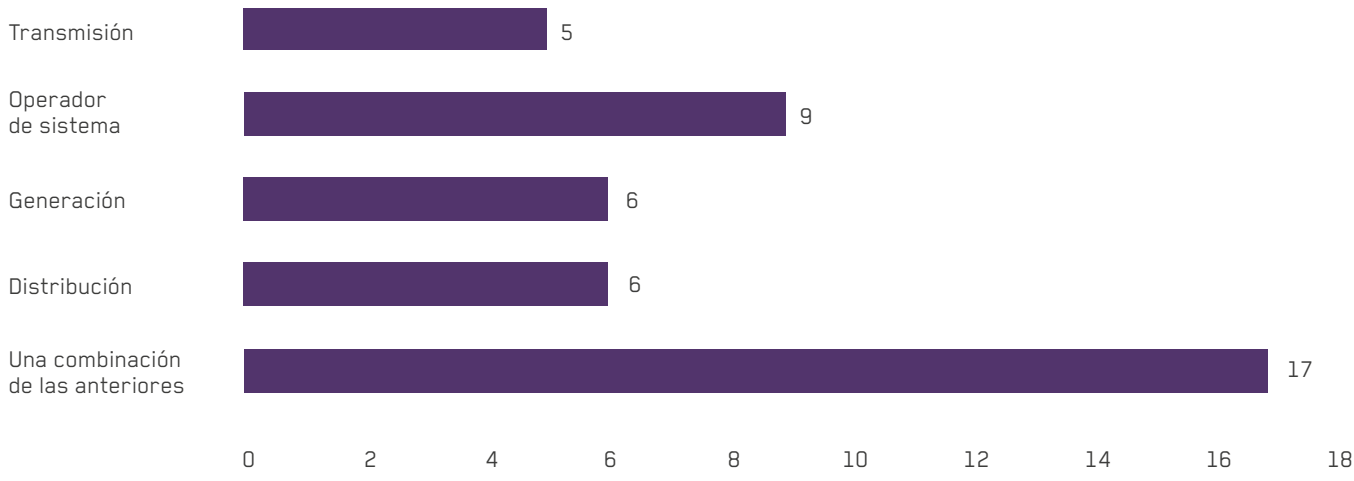


FIGURA 9. Cantidad de participantes del estudio por segmento.

Es importante notar que, de la muestra, el 40% de los participantes se identifican como empresas multisegmento, es decir que no se dedican de manera exclusiva a un segmento concreto de la cadena de suministro. No hay una discriminación específica de a cuáles segmentos específicamente se tiene pertenencia. Los datos analizados van a tener esta consideración a la hora de presentar los resultados.

Podemos identificar también que aunque las empresas del segmento de transmisión suelen ser pocas, se refleja una menor participación en el presente estudio (Ver Figura 10).

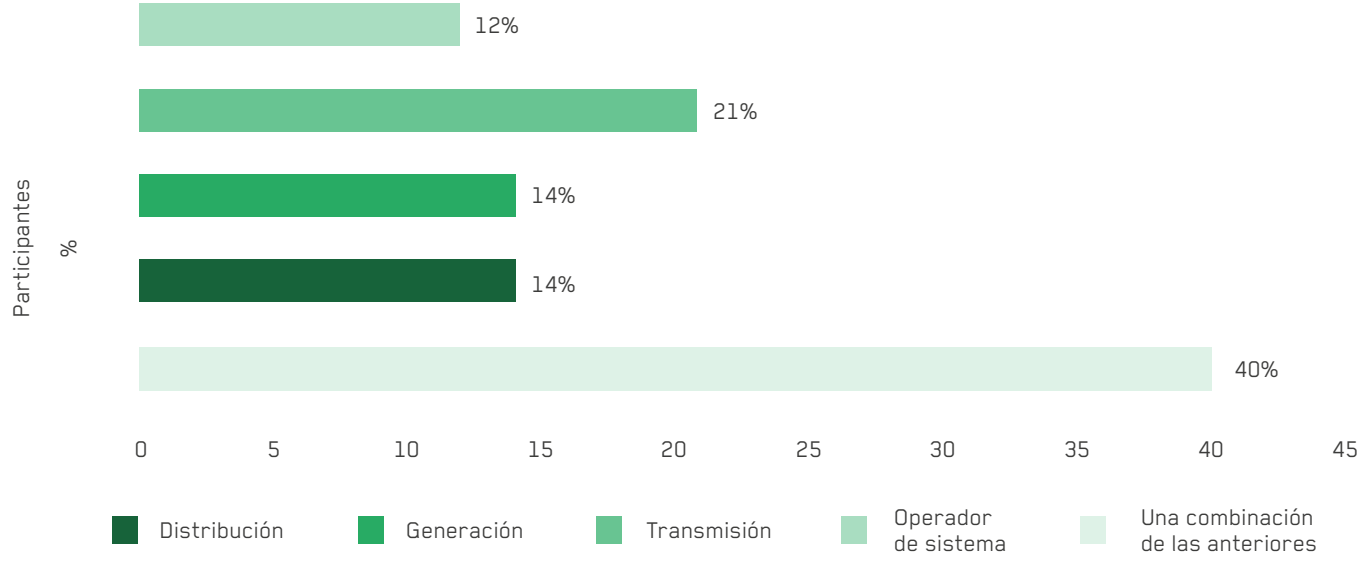


FIGURA 10. Porcentaje de participación por segmento.

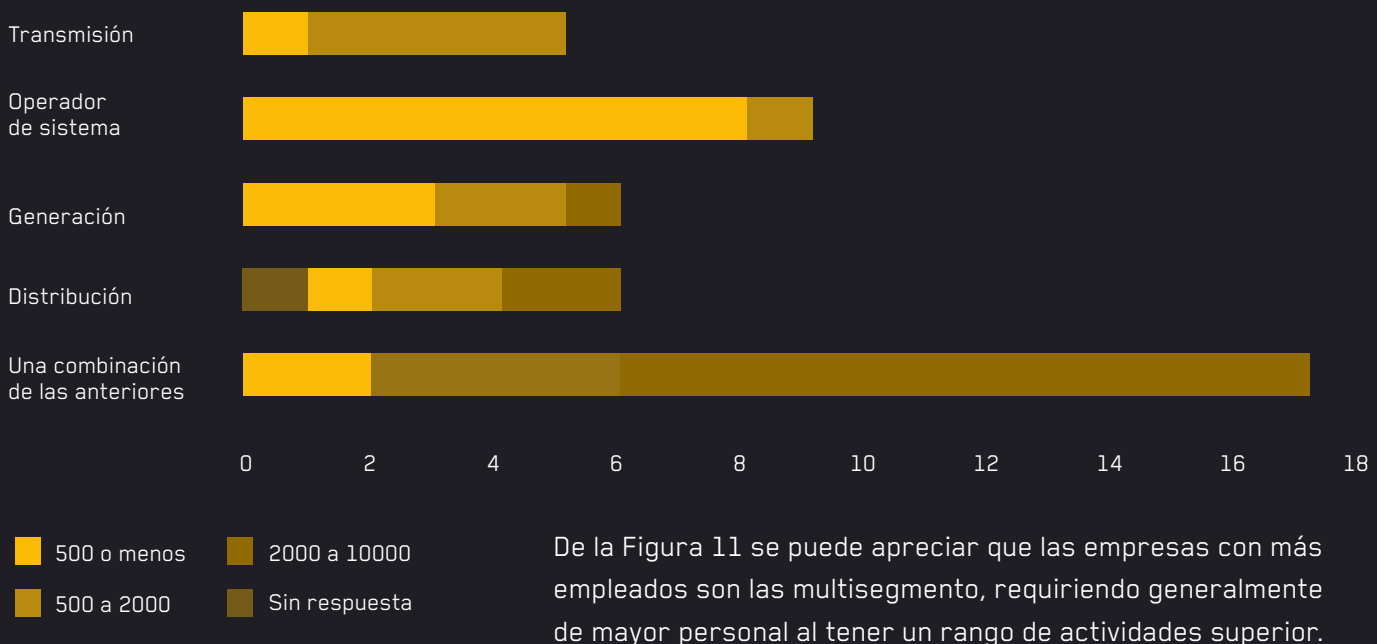
3.3.2 | Por número de empleados

PREGUNTAS ORIENTADORAS

¿Cuántos **empleados tiene** su empresa?

Desde la perspectiva de su tamaño, se consideraron los siguientes factores a evaluar:

- Cantidad de empleados.
- Cantidad de plantas de producción (Generación de energía, estaciones de transmisión, subestaciones, centros de gestión de energía).
- Cantidad de centros de producción (en regiones o países).



De la Figura 11 se puede apreciar que las empresas con más empleados son las multisegmento, requiriendo generalmente de mayor personal al tener un rango de actividades superior.

FIGURA 11. Tamaño de la empresa por cantidad de empleados.

3.3.3 | Por número de plantas o centros de producción

PREGUNTAS ORIENTADORAS

¿Cuántas **plantas de producción tiene su organización?**
(Generación de energía, estaciones de transmisión, subestaciones, centros de gestión de energía)

Cuando se indagó por el tamaño de la empresa por su cantidad de plantas (Figura 12), fue evidente la abstención de gran parte de los participantes a comunicar esta característica.

Sin embargo, nuevamente se aprecia que las empresas multisegmento suelen contar con operación 3 a 5 plantas.

Se puede inferir que los empleados se encuentran uniformemente repartidos en las plantas de acuerdo con sus diferentes sectores. Sin embargo, la limitada participación hace insuficiente la evidencia para concluirlo categóricamente.

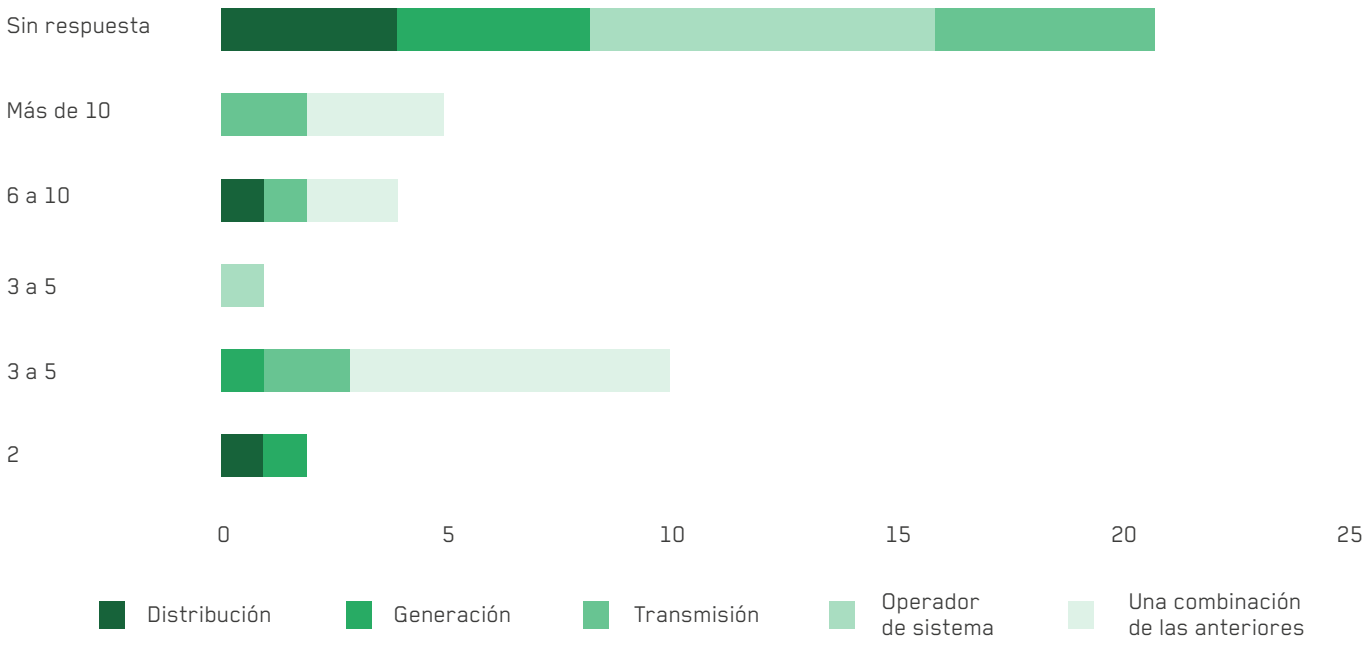


FIGURA 12. Tamaño de la empresa por cantidad de plantas.

3.3.4 | Por regiones o países de operación

PREGUNTAS ORIENTADORAS

Si tiene centros de producción en varias regiones o países, **¿en cuántas regiones tienen centros?**

Al consultar respecto a si las empresas son nacionales o si tiene operación en diferentes regiones o países (Figura 13), se resalta que varias de las empresas identificadas como operadores del sistema no contaban con ningún centro de producción. Esto puede ser derivado de que, por su naturaleza en el proceso no requieren necesariamente centros distribuidos en diferentes regiones o países.

Nuevamente las empresas multisegmento se mostraron con operaciones más amplias donde cuentan con presencia en varias regiones o países. En contraste, se confirma que por su naturaleza las empresas generadoras están mucho más concentradas y no tan dispersas.

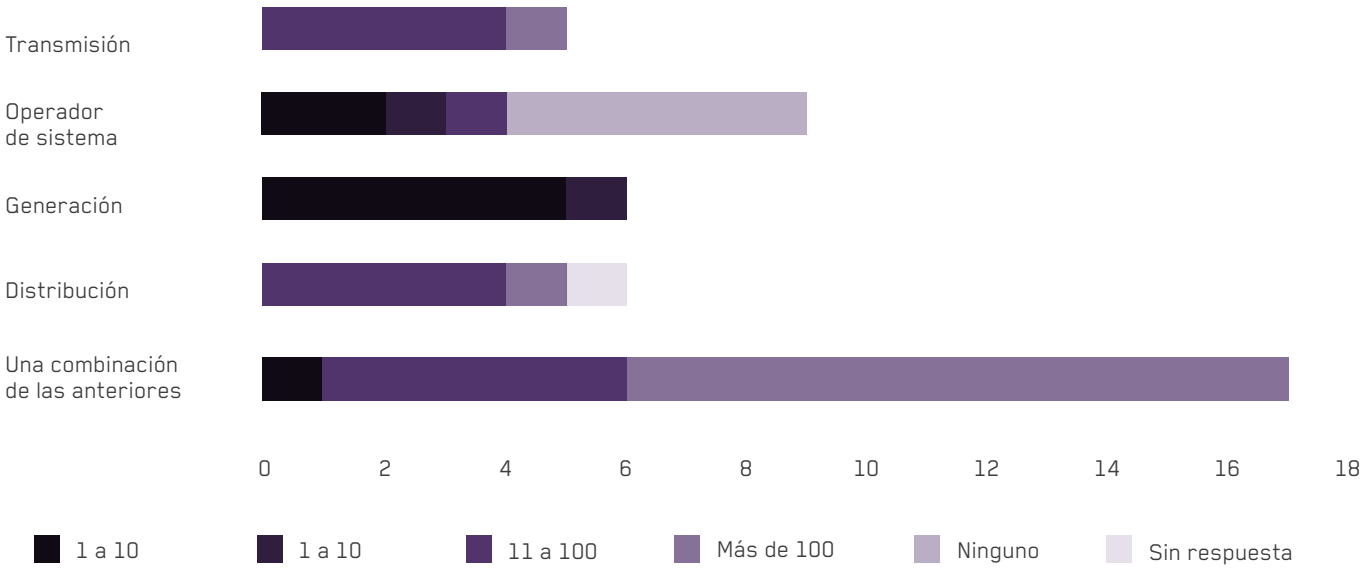


FIGURA 13. Tamaño de la empresa por cantidad de centros de producción.

3.4 | Análisis de datos y hallazgos

El estudio se centra en indagar en los siguientes dominios relacionados con la ciberseguridad y la resiliencia de las organizaciones relacionadas con la cadena de suministro:

Gestión de la cadena de suministro

Gestión de la seguridad lógica

Gestión de las comunicaciones

Gobernanza de la seguridad

Las vulnerabilidades **pueden evitarse o mitigarse** generando capacidades en **las compañías**

Se busca dar un enfoque de riesgos a este análisis, donde los tomadores de decisión puedan conocer el estado y así proyectar las acciones de mitigación.

Se puede considerar el nivel del riesgo como una función de la probabilidad de amenazas y vulnerabilidad, y su impacto a través de las consecuencias derivadas de la explotación de esas vulnerabilidades.

Las vulnerabilidades pueden evitarse o mitigarse generando capacidades en las compañías.

El estudio pretende indagar acerca del conocimiento y percepción de las amenazas, así como del estado de las vulnerabilidades en las organizaciones del sector y su impacto potencial, tanto en la propia industria como en la sociedad en su conjunto.

Este enfoque busca entender el grado de preparación y concienciación con el que cuentan los hoy responsables de la ciberseguridad.

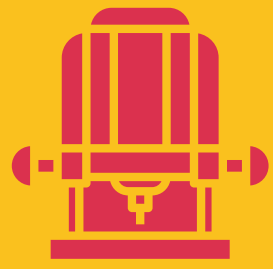
Para poder solucionar un problema, lo primero es reconocer que existe, para ello se exploran aspectos en cada uno de estos dominios como una primera aproximación para poner en común el estado de la ciberseguridad.

Está previsto que futuras ediciones de la encuesta profundicen en estos dominios de seguridad y analicen otros nuevos que permitan aumentar el grado de conocimiento del sector y, con ello, facilitar el consenso acerca de recomendaciones que puedan ser útiles para mejorar el estado de la ciberseguridad TI e industrial.

3.4.1 | Cadena de Suministro: Proveedores de Tecnologías de Operación

PREGUNTAS ORIENTADORAS

¿Cuál es el tipo de su **proveedor principal de equipos de tecnología operacional (TO)?**



Toda organización requiere definir la cadena de suministro para garantizar que su operación sea gobernable.

En este sentido, se ha indagado acerca de cómo adquieren los equipos de Tecnología Operacional de los participantes.

Al momento de la adquisición de equipamiento, hay una gran variedad de opciones utilizadas por la industria, como puede reflejarse por los resultados mostrados en la Figura 14.

Se aprecia que, de manera casi uniforme, las empresas de cada segmento adquieren sus equipos directamente de los fabricantes o bien de mayoristas, lo que debería permitirles acceder al soporte directo del fabricante. Precisamente, para revisar cómo las empresas del sector han contratado el soporte para el equipamiento adquirido, se les preguntó de manera separada por el soporte de primer y segundo nivel, para luego preguntar por el soporte de tercer y cuarto nivel.

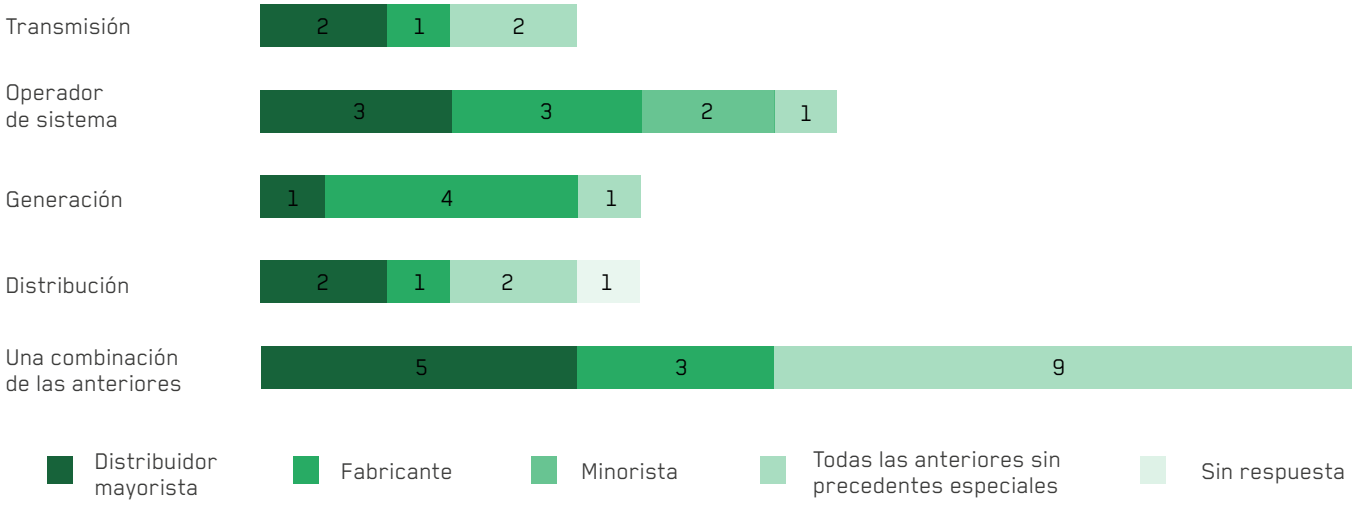


FIGURA 14. Tipo de proveedor de equipos de tecnología operacional

3.4.2 | Cadena de Suministro: Proveedores de Soporte de Primer y Segundo Nivel

PREGUNTAS ORIENTADORAS

¿Quién **proporciona apoyo** de primer y segundo nivel a su **equipo de TO**?

Un aspecto para resaltar en los resultados es que las empresas prefieren confiar en los empleados internos formados para dar el soporte de primer y segundo nivel. Aunque algunos pueden contratar con el fabricante o con terceros, el contar con su propio personal cualificado es la opción más común.

Esto puede acarrear problemas si no hay políticas relacionadas con la rotación o el cambio de personal, esta capacidad puede desaparecer de la organización. Asimismo, esta situación tampoco garantiza que los empleados estén actualizados y que mantengan las destrezas necesarias para dar solución a los problemas.

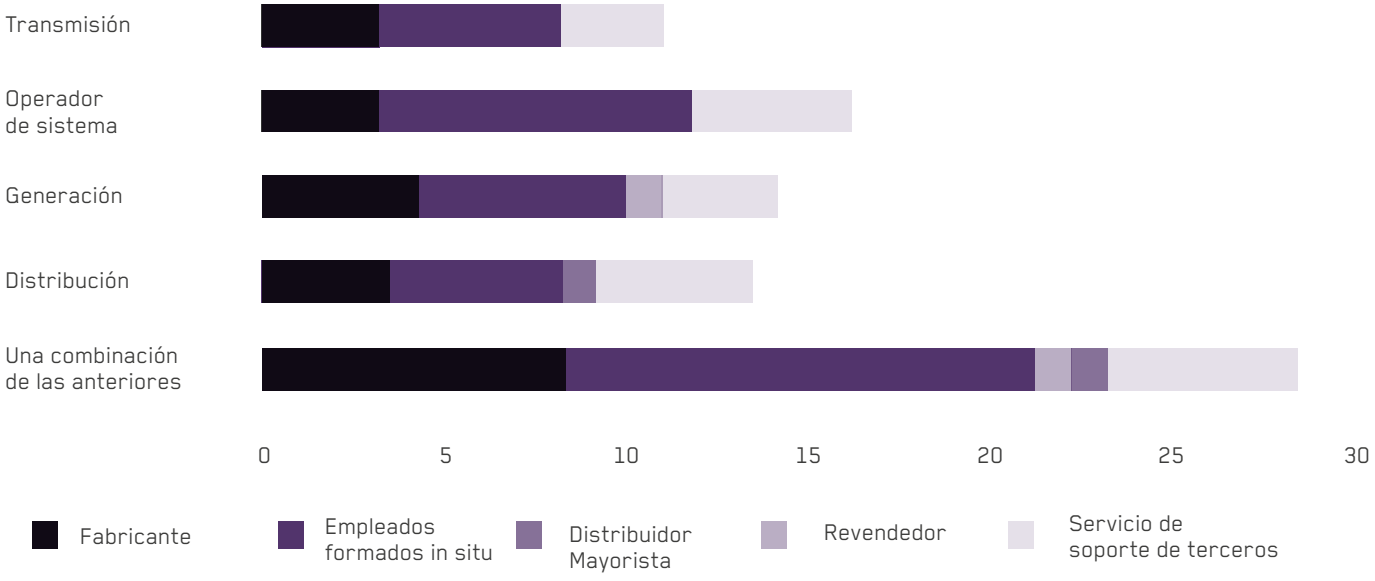


FIGURA 15. Soporte de primer y segundo nivel de las Tecnologías de Operación

3.4.3 | Cadena de Suministro: Proveedores de Soporte de Tercer y Cuarto Nivel

PREGUNTAS ORIENTADORAS

¿Quién provee **soporte** de tercer y cuarto nivel a su **equipo de TO?**

A la hora de contratar el soporte de tercer y cuarto nivel (Figura 16), las empresas prefieren confiar en el fabricante y los distribuidores mayoristas. Los problemas que deben ser resueltos a este nivel requieren de equipos mucho más especializados y con una mayor dedicación. Sin embargo, la opción de cualificar a sus propios empleados para atender los incidentes de mayor gravedad sigue siendo una prioridad.

La priorización de los esfuerzos en personal interno puede entrañar un riesgo para lograr resolver situaciones críticas, al ser parte del proceso.

Una situación que entraña una gran gravedad para esa industria en particular y para la sociedad en general es que algunas empresas no cuentan con soporte de tercer y cuarto nivel. Esto las deja expuestas ante situaciones críticas que no pueden resolver de manera interna y para las que no tienen a quién acudir.

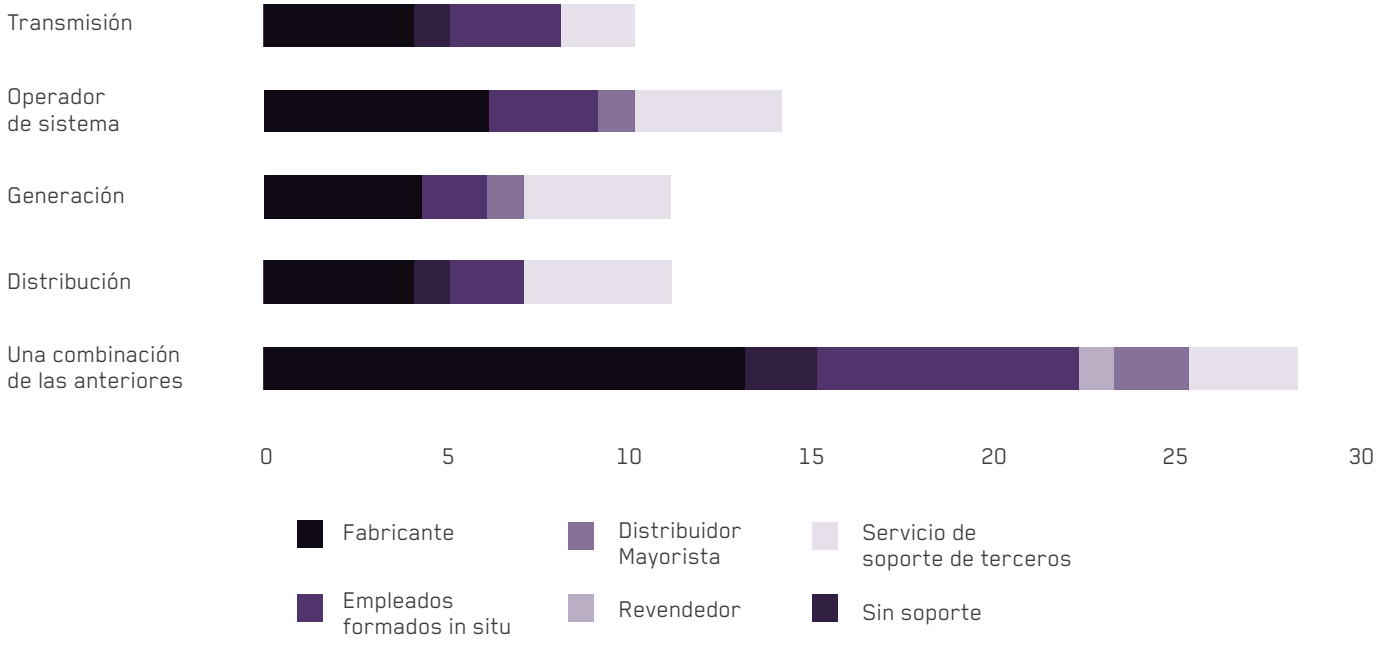


FIGURA 16. Soporte de tercer y cuarto nivel equipo de las Tecnologías de Operación.

Todo lo anterior origina que se incumpla el principio de las Tres Líneas de Defensa para una Gestión del Riesgo y Control, que requiere una segregación de funciones entre los 3 grupos siguientes:

Las funciones que supervisan los escenarios de riesgo.

Las funciones que son propietarias de los escenarios de riesgo y los gestionan.

Las funciones que proporcionan un aseguramiento independiente.

3.4.4 | Gestión de las Comunicaciones

PREGUNTAS ORIENTADORAS

- ¿Mantiene **su organización** una separación entre sus **redes de control** y de negocios? **(Figura 17)**
- ¿Cómo **separa su** organización sus **redes operativas?** **(Figuras 18 y 19)**
- ¿Las **redes de TO** de su organización están **conectadas a Internet?** **(Figuras 20 y 21)**
- ¿Su organización mantiene una **VLAN dedicada para backup?** **(Figura 22)**
- ¿Su organización **mantiene una VLAN de seguridad dedicada?** (para todos los dispositivos de seguridad) **(Figura 23)**

Un aspecto básico para indagar es si las empresas tienen segmentadas sus redes, de manera puntual, si existe separación entre sus redes informáticas de TO y TI.

En la Figura 17 se aprecia lo que contestaron las empresas pertenecientes a cada segmento de la cadena de suministro.

Es **importante notar** que la segmentación **permite** el confinamiento del **tráfico y la gestión** de la comunicación que pasa por los **diferentes conductos.**

Aunque es notorio que el uso de la segmentación de las redes como buena práctica en ciberseguridad es común a los diferentes segmentos, en entornos industriales es mucho menos frecuente, a pesar de su elevada criticidad. Es importante notar que la segmentación permite el confinamiento del tráfico y la gestión de la comunicación que pasa por los diferentes conductos. Al poder definir el uso de cada VLAN, se puede definir reglas de QoS en los protocolos 802.x y garantizar la menor latencia posible.

23 de las empresas indican que en sus instalaciones cuentan con redes independientes, es decir, que no están conectadas a las demás instalaciones de la empresa. A su vez, que estas redes están segmentadas internamente, garantizando una separación entre TO y TI.

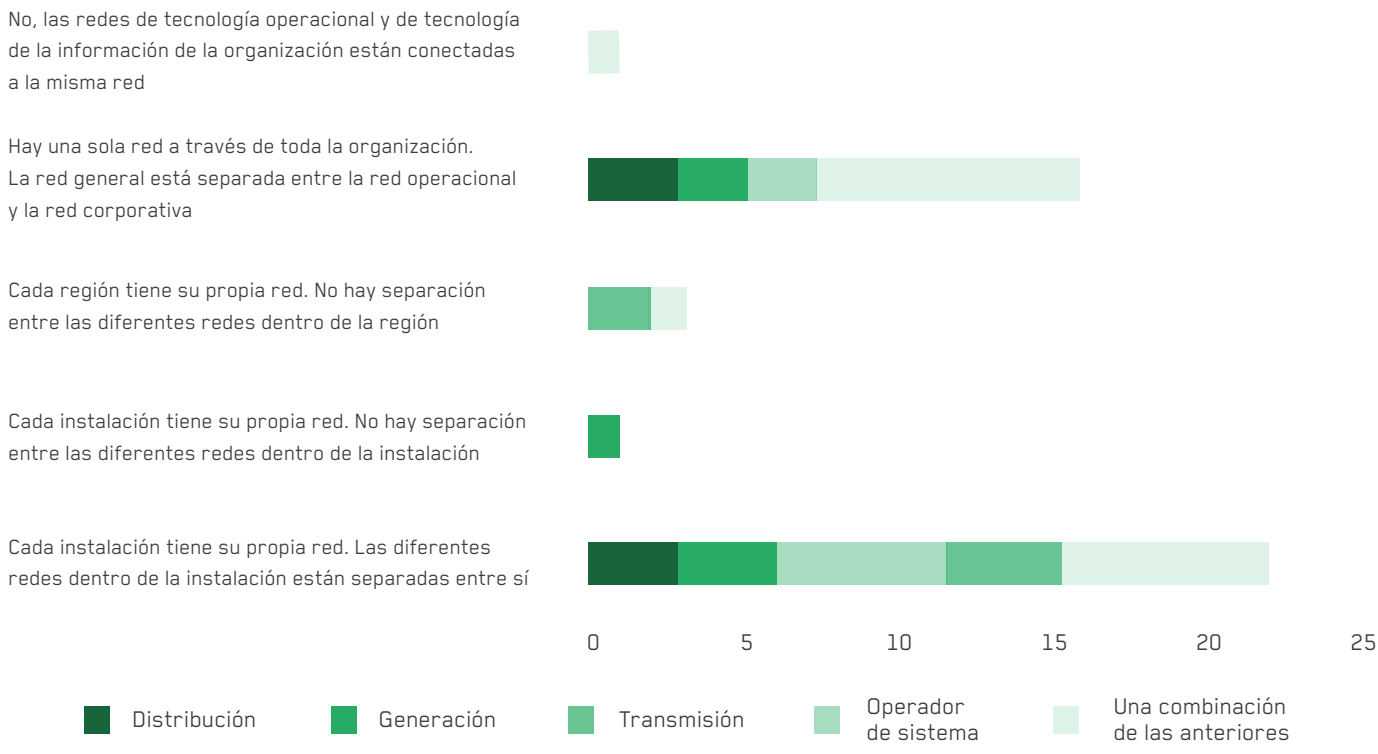


FIGURA 17. Separación entre redes de control y de negocios.

Lo importante a resaltar es que el 37% de las empresas tienen una sola red común a todas sus instalaciones y que tan solo en donde se requiere, se hace una separación entre las redes industriales de TO y las redes de información TI. Esto puede aumentar la probabilidad de que el incidente en una de sus instalaciones puede propagarse a las demás, aumentando con ello notablemente el impacto. Tener una red común que contenga el tráfico TI y TO puede provocar latencias elevadas, y que la gestión de los diversos protocolos sea poco óptima.

En la Figura 18 se muestra cómo son las redes segmentadas.

Llama la atención que las empresas de los diferentes sectores no hayan contestado a la pregunta formulada, lo que puede indicar que no tienen manera alguna de segmentación de las redes. En contraste, se aprecia que quienes sí hacen la segmentación puedan hacerlo siguiendo unas buenas prácticas.

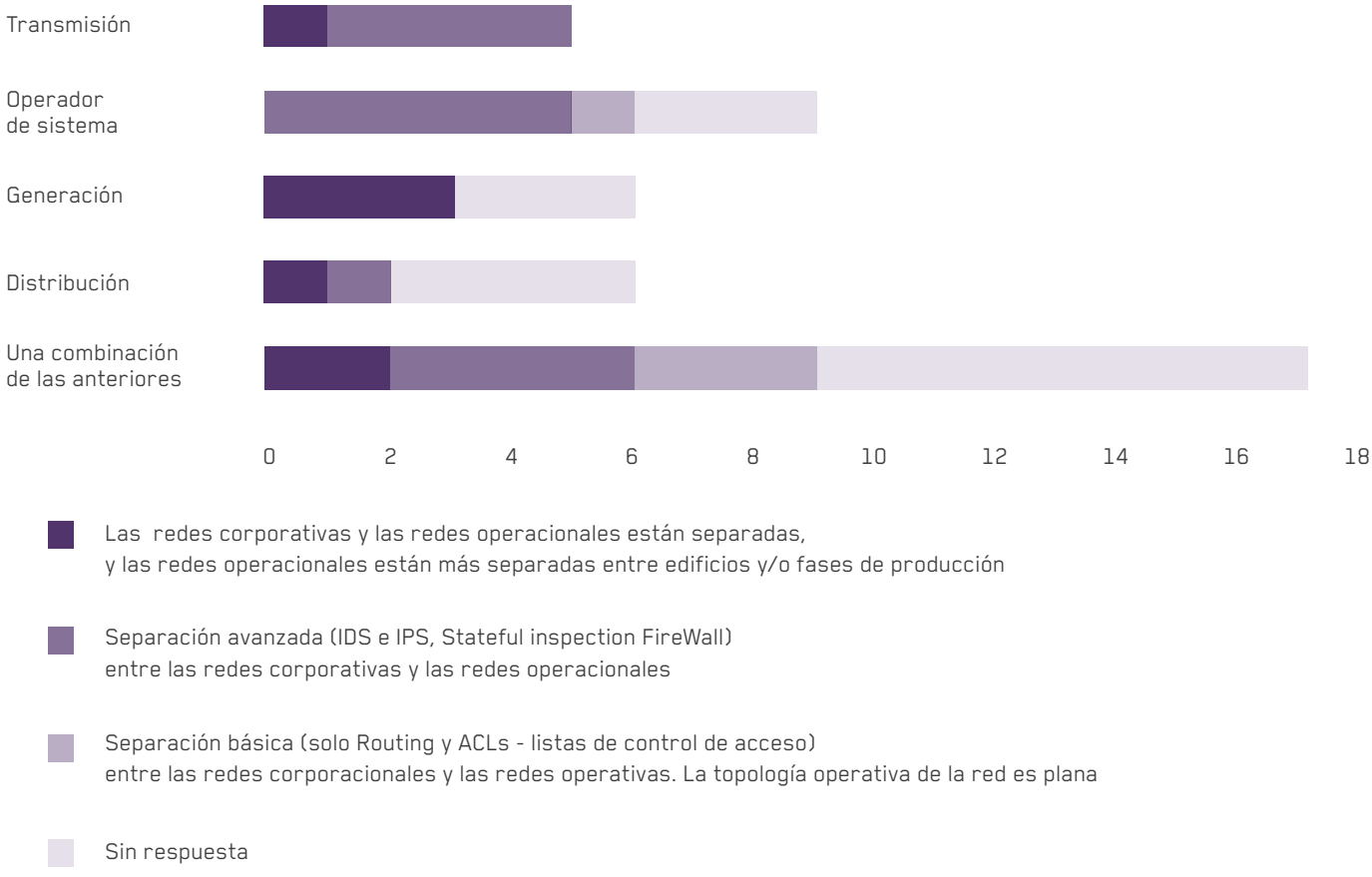


FIGURA 18. Separación de las redes operativas.

Las amenazas relacionadas con el acceso indebido a los sistemas, la propagación de malware y ramsonware pueden ser mitigadas con la segmentación eficiente de las redes. Pero al compartir elementos de red y tráfico, las amenazas propias de TI pueden propagarse y contagiar las redes TO.

Para ahondar es este punto, en la Figura 19 se representa la relación entre quienes segmentan y el tipo de segmentación que es aplicada. De aquí se puede

inferir que quienes segmentan, suelen usar todo un conjunto de técnicas para garantizar que dicha segmentación aísle las diferentes redes, y en complemento que la ausencia de respuesta está relacionada con la no segmentación de sus redes TI y TO.

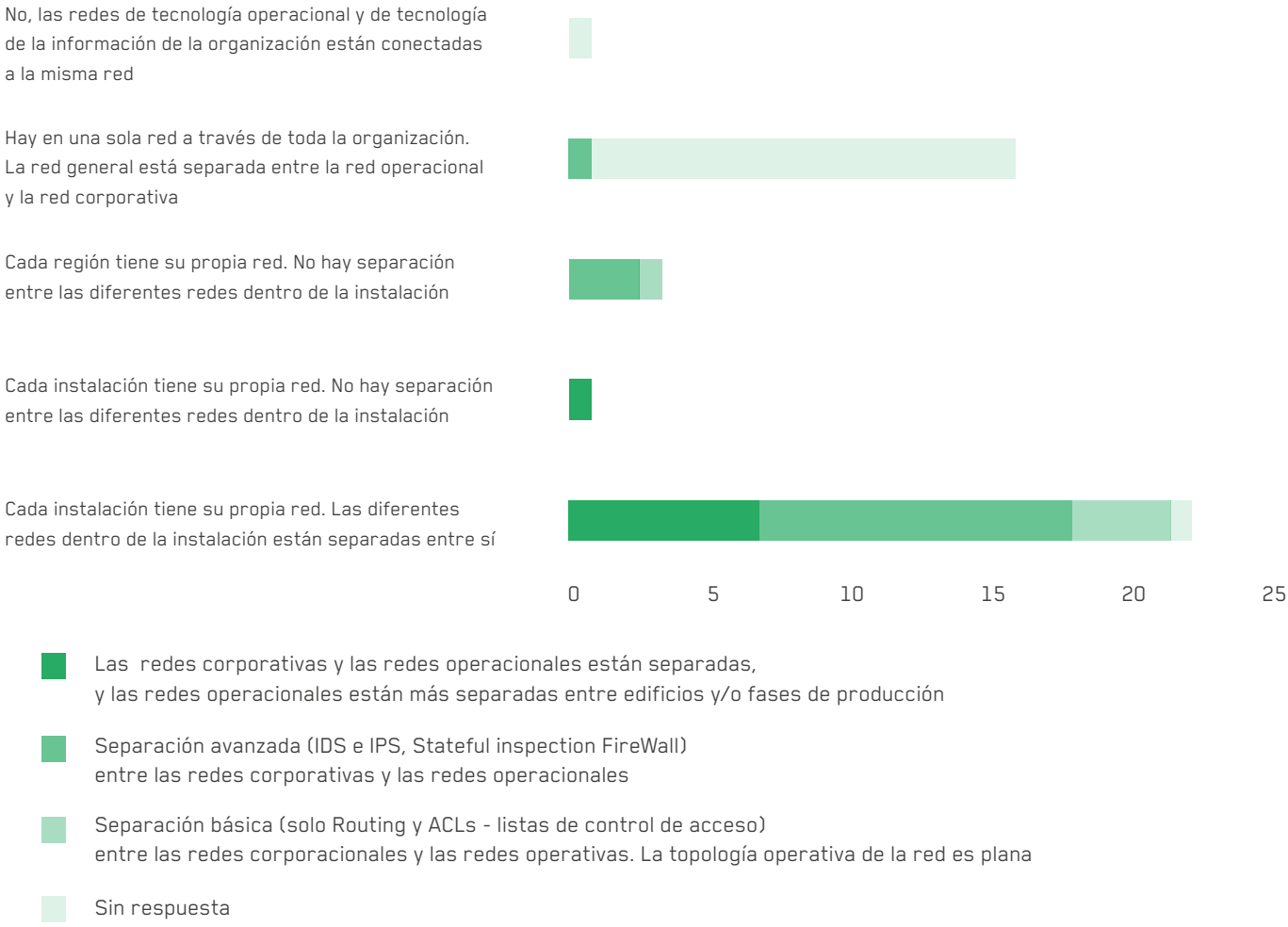


FIGURA 19. Relación entre segmentación y las técnicas.

Al indagarse si la red TO estaba conectada a Internet se aprecia que en promedio el 50% de las redes TO no están conectadas a Internet (ver Figura 20). Hay una excepción para las empresas del segmento transmisión, que en su totalidad tienen conectividad a Internet a través de la red TI. Para los segmentos de empresas de distribución y combinación de las anteriores, indican que tienen salida directa a internet. Esto implica la exposición de su infraestructura a amenazas externas.

Es importante que se valore la necesidad que las redes TO tengan acceso directo o indirecto a internet. Esto genera una ampliación de la superficie de ataque y expone a las organizaciones de manera directa a ataques externos.

FIGURA 20. Redes TO conectadas a Internet.

Si se examina la conexión a internet con la segmentación de las redes TO, se aprecia una relación preocupante (Ver Figura 21). Al no estar segmentada la red, la exposición hacia internet se hace por medio de la red TI principalmente. Se presenta un caso donde a pesar de tener completa segmentación de las redes y sus instalaciones, hay salida directa a internet de la red TO. También se presenta un caso donde la separación es mínima y aun así se expone directamente a internet.

Si no hay una adecuada segmentación y una clara exposición a internet, un ataque a la infraestructura TI puede comprometer rápidamente la infraestructura TO. Un atacante externo, en su proceso de reconocimiento, puede darse cuenta que puede acceder a la red TO por medio de la red TI, y esto le facilita ampliamente las opciones para vulnerar los sistemas.

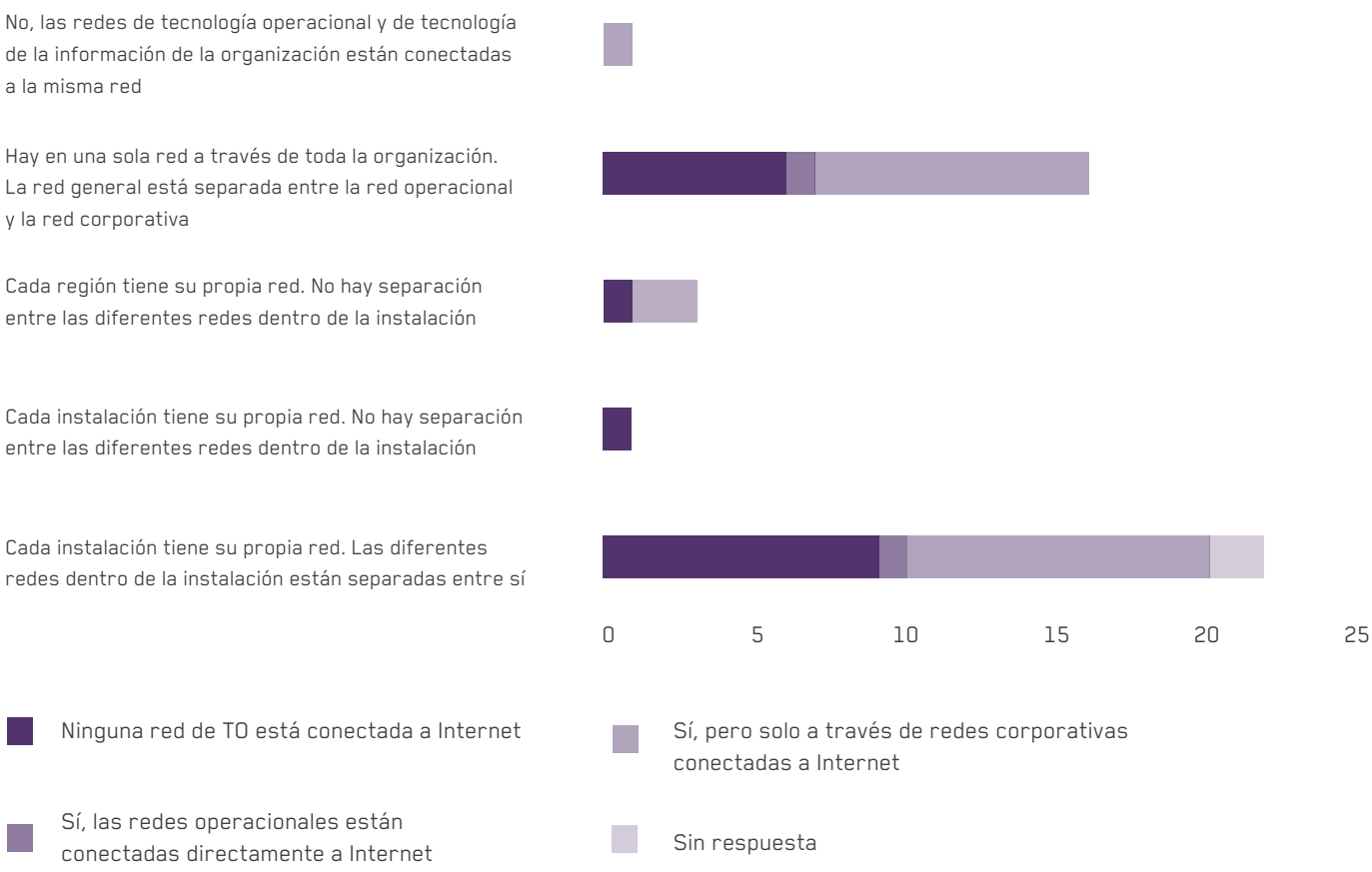


FIGURA 21. Relación entre la separación de las redes y su conexión a internet.

Una buena práctica recomendada es establecer segmentos especializados que permitan priorizar el tráfico. En la Figura 22 se muestra el uso de la VLAN para backup y en la Figura 23 el uso de la VLAN para seguridad.

Las empresas del segmento de transmisión no tienen una VLAN dedicada para backup. Quienes no tienen la VLAN dedicada, pero tienen dispositivos de backup, estos están dispersos en diversas VLAN o en una única con permisos de acceso especiales.

Tener VLAN dedicada al tráfico de los componentes de backup permite que este no afecte el tráfico ordinario. Este tráfico suele tener picos que responden a las acciones definidas por las políticas de respaldo.

Un comportamiento semejante se observa al indagar acerca de las VLAN dedicadas a seguridad. Nuevamente las empresas de transmisión no cuentan con una VLAN dedicada, y quienes si tienen los dispositivos de seguridad, están en VLAN diferentes o en la misma, pero con funciones adicionales.

Quienes no tienen la VLAN dedicada, pero que tienen **dispositivos de backup**, estos están dispersos en **diversas VLAN** o en una única **con permisos** de **acceso especiales.**

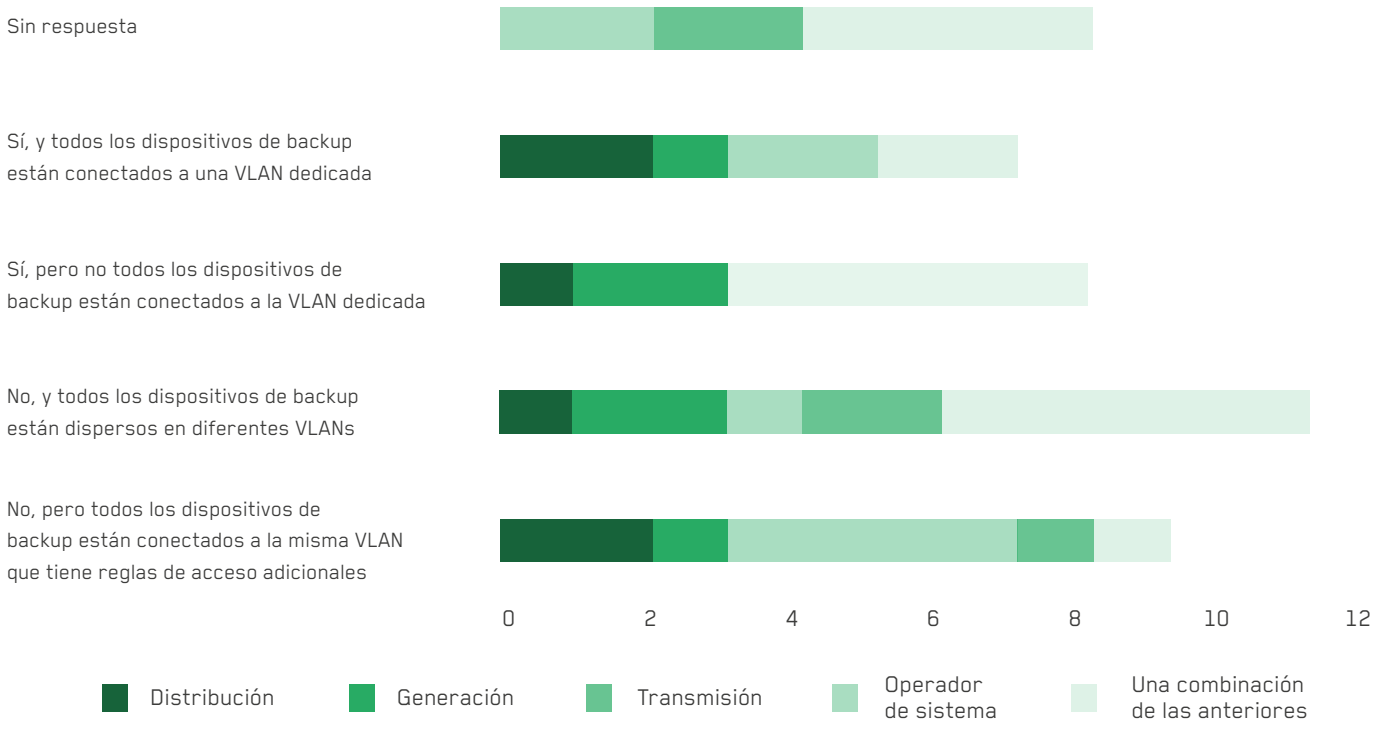


FIGURA 22. Uso de VLAN de backup.

Contar con una VLAN dedicada para la seguridad garantiza que el tráfico relacionado con la recolección de los registros del sistema y de las demás herramientas de monitoreo y medición, no contamine el tráfico ordinario de TO. De la misma manera, la gestión de las herramientas de seguridad no requiere que se tenga acceso a los procesos industriales, permitiendo además hacer una limitación al control de acceso a la red TO.

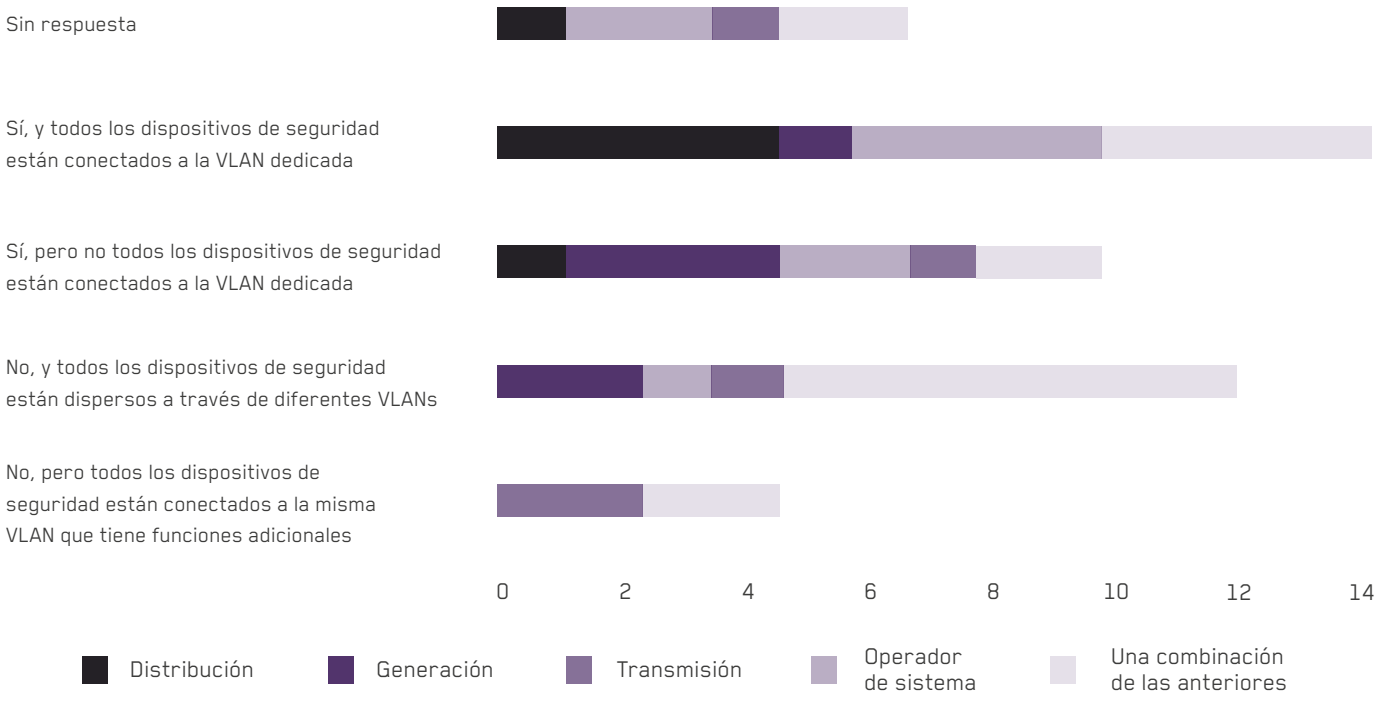


FIGURA 23. Uso de VLAN dedicada a seguridad.

3.4.5 | Gestión de la red TO

PREGUNTAS ORIENTADORAS

- ¿Su organización mantiene **Control de Acceso a la Red** (Network Access Control, NAC) en su **red operacional?** (Figura 24)
- ¿Cómo se **configura el NAC** (Network Access Control) en sus redes operacionales? **(Figura 25)**
- ¿Su organización **mantiene una conexión remota** a sus redes **operacionales?** (Figura 26)
- ¿Mantiene su **organización** una conexión remota a sus **redes corporativas?** (Figura 27)
- ¿Cuál de las siguientes **opciones** describe los **dispositivos de red** remotos y las **políticas de administración** de su organización? **(Figuras 28 y 29)**
- ¿Qué **controles de seguridad** utiliza su organización para **proteger** sus **redes inalambricas (Wi-Fi)** manejando **tecnología operacional?** (Figura 30)

Así como en las redes de TI se debe gestionar los dispositivos conectados, se indaga el mismo requerimiento para las redes TO. En la Figura 24 se aprecia la capacidad de gestión de la red TO. Solo una empresa del segmento de generación indicó que no tenía gestión de los dispositivos de red. En general se reconoce que no todos los dispositivos conectados a la red TO están siendo gestionados.

Tener una gestión de los dispositivos y el descubrimiento de estos, permite reconocer cuales dispositivos están conectados de manera permanente y cuales se conectan de manera frecuente. Establecer este monitoreo permite generar alertas cuando dispositivos nuevos se conectan y evaluar así su legitimidad.

Cerca de un 65% de las empresas **reconocieron** que no cuentan con NAC (control de acceso a la red) **para su red TO**

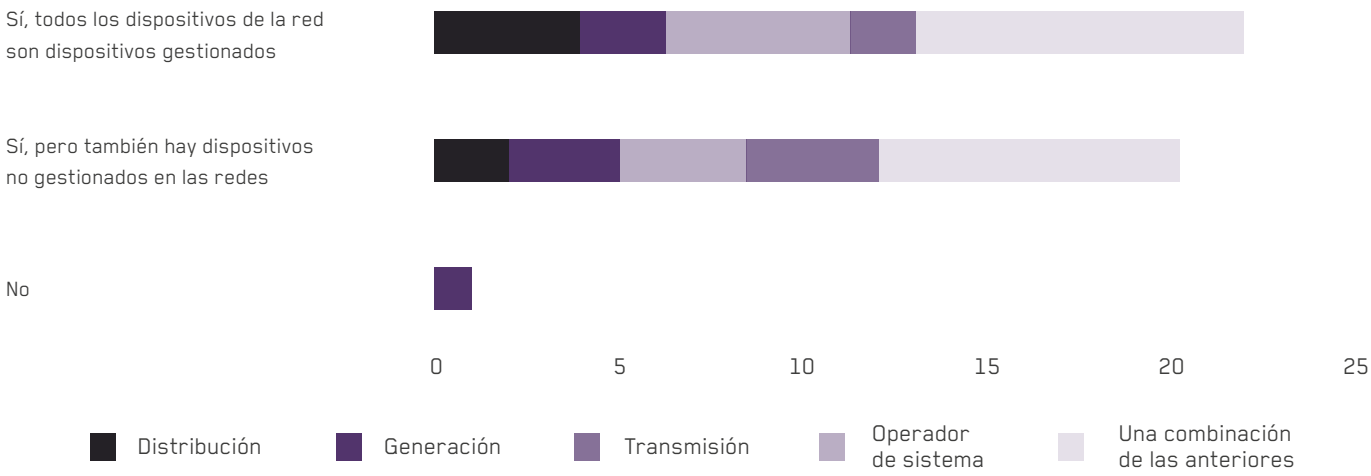
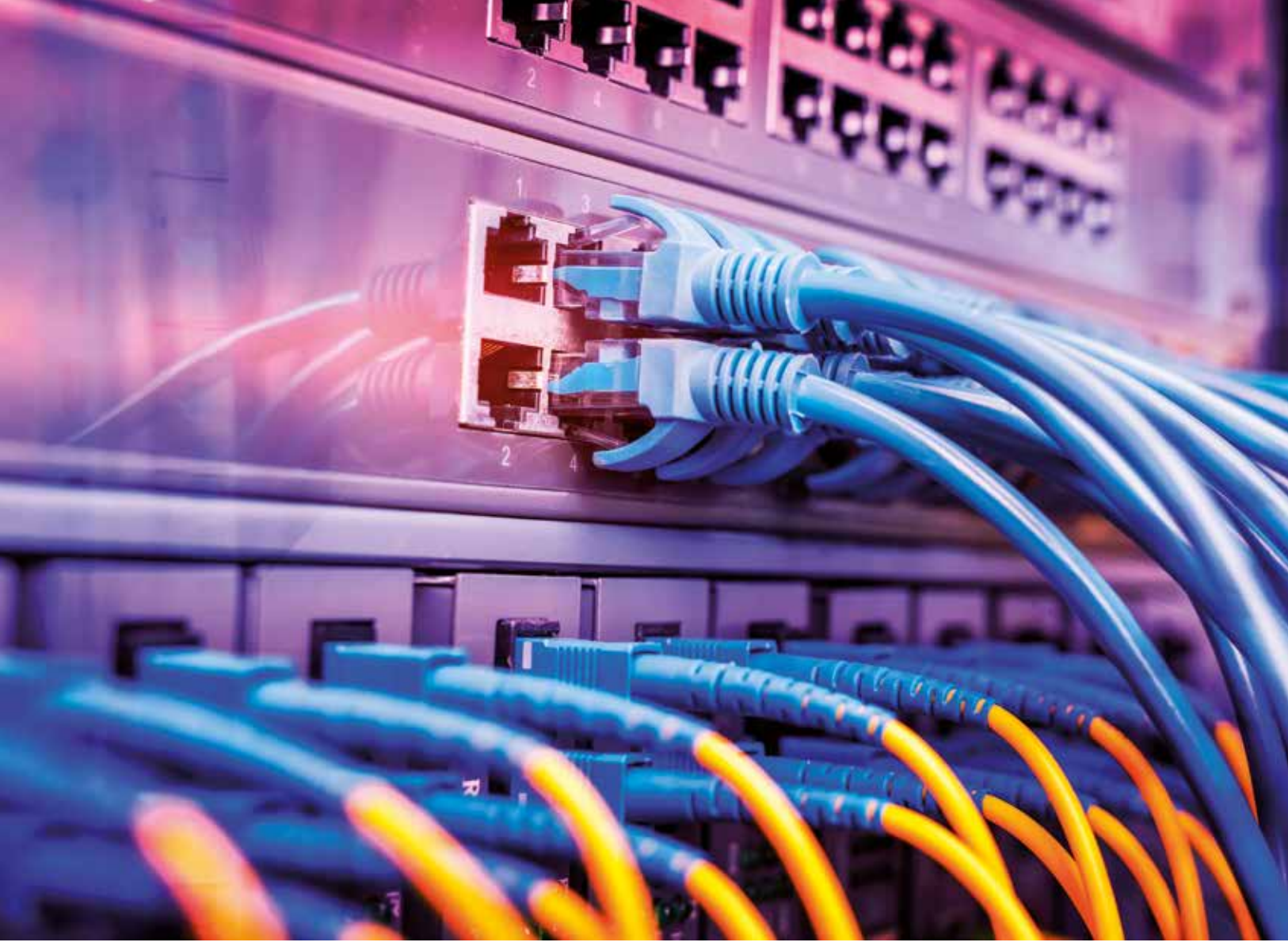


FIGURA 24. Gestión de dispositivos de red.

Cerca de un 65% de las empresas reconocieron que no cuentan con NAC (control de acceso a la red) para su red TO. Nuevamente, las empresas del segmento de generación reconocen que en su totalidad no cuentan con esta medida de protección. Combinado esto con el hecho de no contar con una gestión completa de los dispositivos de red, hace que un equipo comprometido pueda llegar a conectarse a la red TO de manera inadvertida y ser así un vector de entrada de algún tipo de ataque.

Al contar con un NAC, se pueden establecer reglas para que solo equipos que cumplan ciertos perfiles de seguridad tengan el privilegio de conexión. Esto puede ser, que su dirección MAC se corresponda con una lista de dispositivos autorizados, o que el dispositivo cumpla unos requisitos mínimos de autoprotección, como tener actualizado su *firmware*, su sistema operativo, que cuenten con solo unos pocos puertos abiertos.



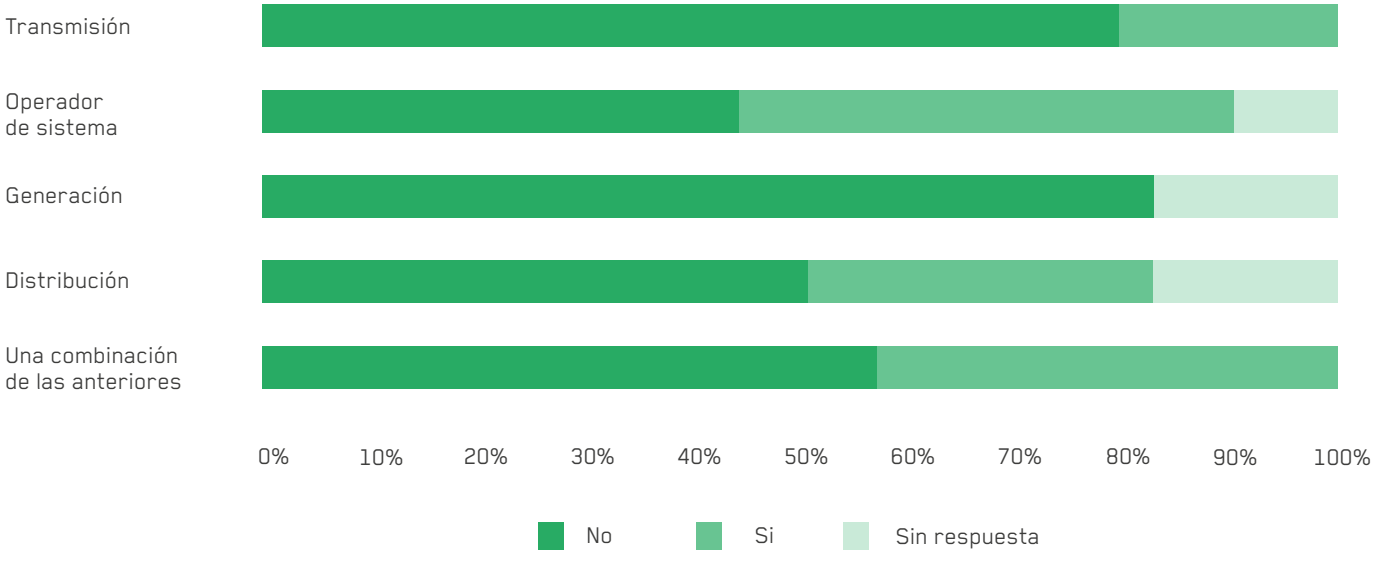


FIGURA 25. NAC en la red TO.

Así como en la sección anterior se preguntaba acerca de si la red TO tenía salida a internet, aquí se indaga acerca de si hay acceso remoto a la misma red. Casi la mitad de las empresas de todos los sectores no respondieron a la pregunta.

Exceptuando las empresas del segmento de distribución, las demás empresas reconocen que es posible establecer conexiones remotas desde internet.

Es importante evaluar la necesidad de contar con acceso remoto a la red TO. La operación en las plantas suele ser 7x24x365 de tal manera que siempre habrá personal de guardia en las instalaciones. Si hay necesidad imperiosa de acceder de manera remota, debería garantizarse por medio de VPN.

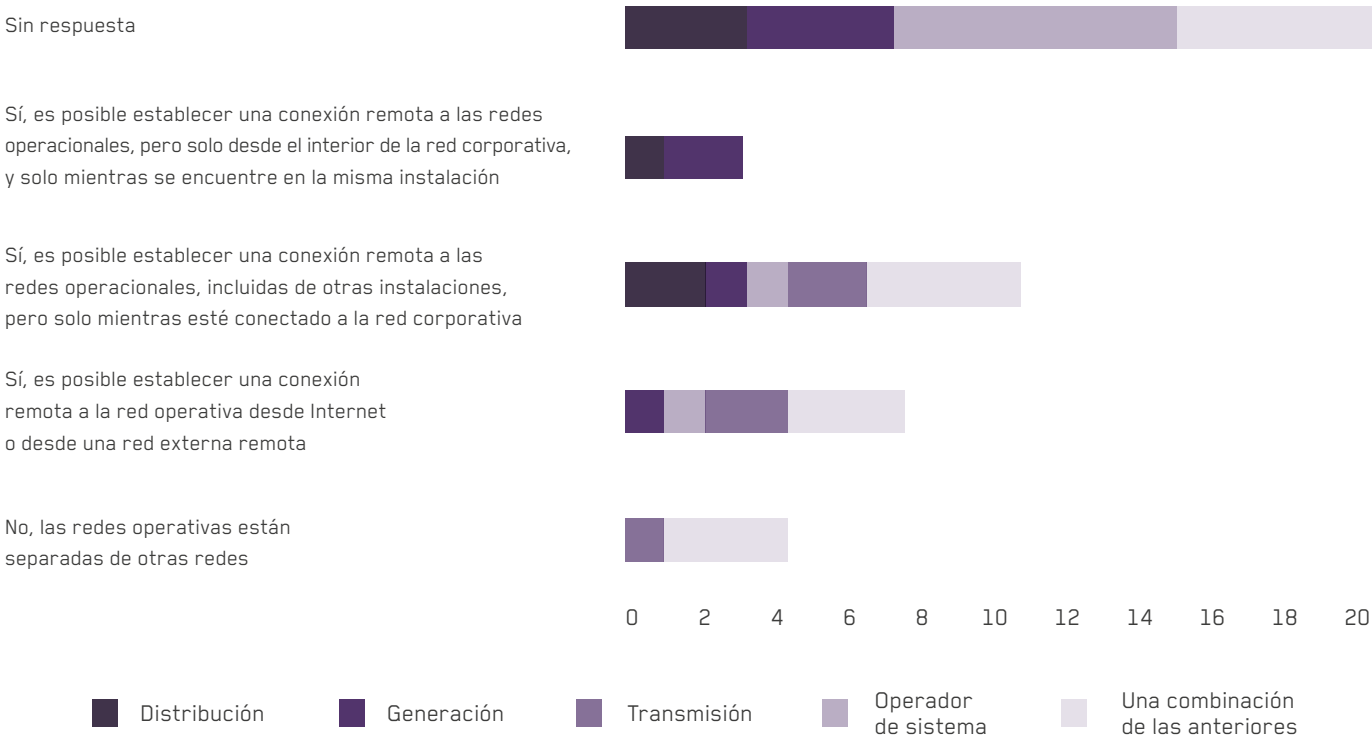


FIGURA 26. Acceso remoto a la red TO.

Respecto al acceso remoto a las redes TI, las empresas de todos los sectores reconocen que pueden tener acceso remoto a través de internet. Los operadores del sistema y de transmisión indican que no tienen reglas que limiten el acceso remoto.

Para los casos en los cuales no hay segmentación de redes o esta es muy débil, es importante limitar también esta posibilidad para las redes TI. El acceso remoto debe configurarse para que se haga por medio de VPN y se implementen múltiples factores de autenticación (algo que sé, algo que tengo y algo que soy).

Los **operadores del sistema** y de transmisión indican que **no tienen reglas que limiten** el acceso remoto.

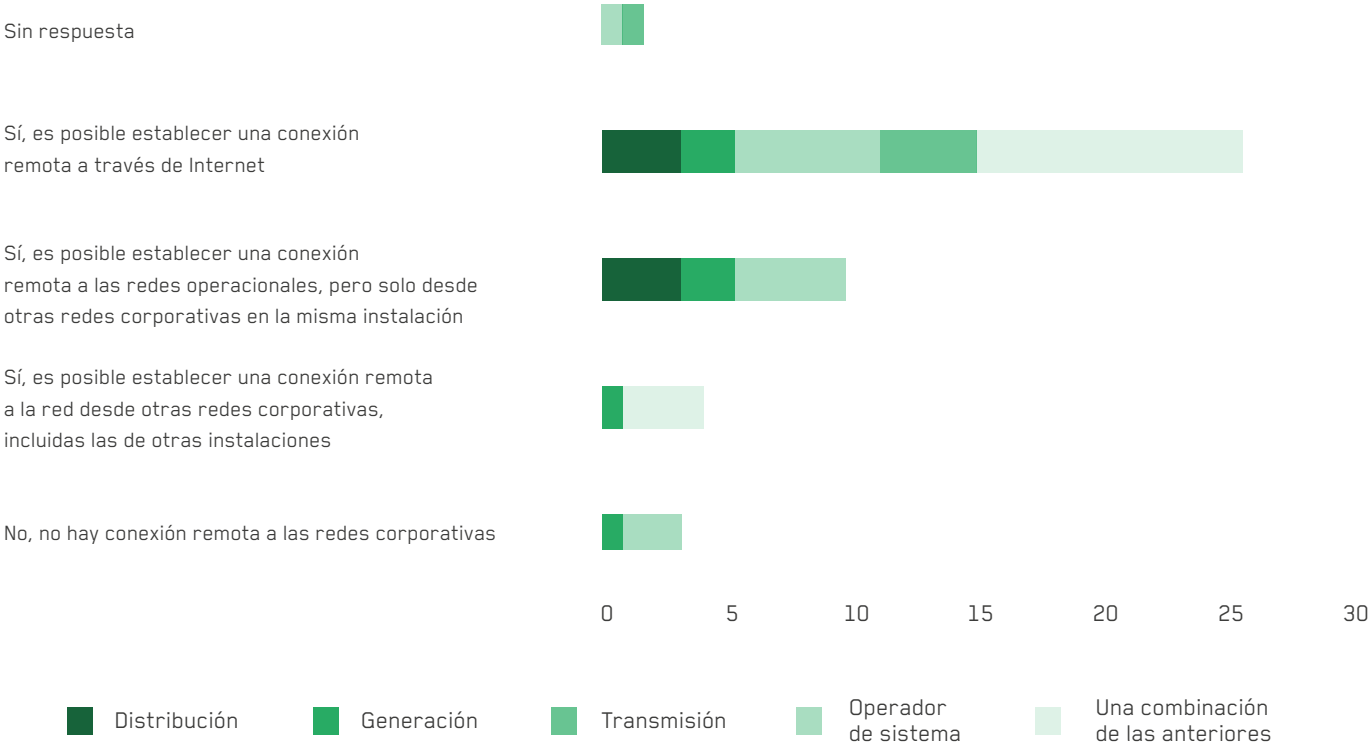


FIGURA 27. Acceso remoto a TI.

La gestión remota de los dispositivos de red es también un aspecto crítico para evaluar. En la Figura 28 se describe cuáles dispositivos de red son gestionados remotamente. Se resalta que empresas de los segmentos de generación, operación del sistema y transmisión cuentan con políticas que establecen que ningún dispositivo de red puede ser administrado remotamente.

Es importante considerar las diversas zonas de seguridad en las que se puede dividir la infraestructura TO y en cada una de ellas determinar los equipos de misión crítica y definir para ellos las políticas de gestión adecuadas. Toda gestión remota debe garantizar cifrado de canal y cifrado de mensaje, así como múltiples factores de autenticación.

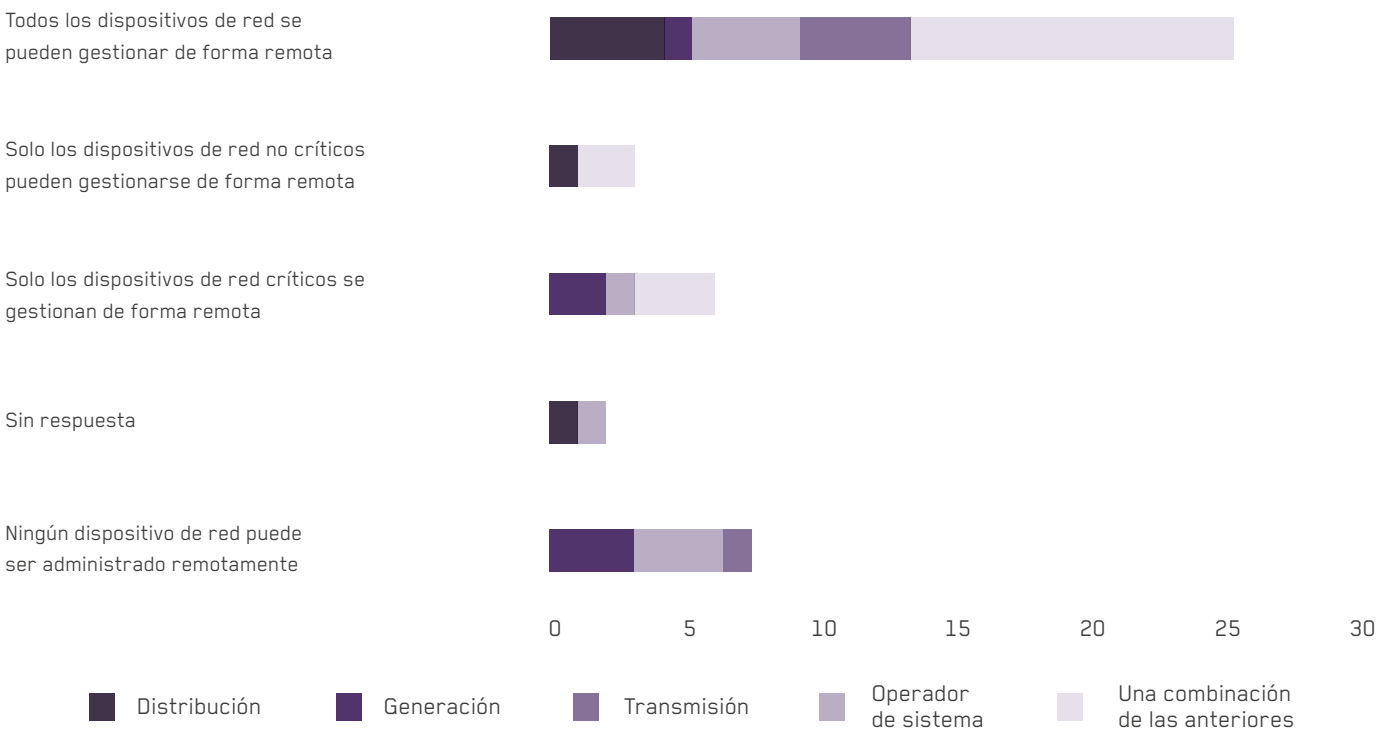


FIGURA 28. Política de gestión de dispositivos de red remotos.

La gestión de los dispositivos de red se realiza por medio del protocolo SNMP (Ver Figura 29). En su versión 3 se incorporan características de seguridad que no eran consideradas en las versiones previas, sin embargo, su adopción en el mercado ha sido muy lenta. Se aprecia que, a excepción del segmento de generación, todos los demás usan aún dispositivos con SNMPv1, pero en todos los casos, la implementación de SNMPv3 está presente. Es usual que convivan en la misma infraestructura dispositivos con protocolos en las tres versiones.

Este es uno de los aspectos más difíciles de controlar en una red TO, debido a que su infraestructura no suele renovarse frecuentemente, suelen convivir dispositivos muy antiguos con otros modernos. Por ello es importante en las acciones de tratamiento del riesgo considerar los controles compensatorios que garanticen la seguridad de la operación en los dispositivos que

Es importante en las **acciones de tratamiento del riesgo considerar** los **controles** compensatorios que **garanticen la seguridad** de la **operación** en los **dispositivos** que están por fuera de su **ciclo de vida**

están por fuera de su ciclo de vida. Aunque en la actualidad el protocolo SNMP en su versión 3 ya incorpora medidas de seguridad que no eran consideradas en sus versiones previas, su adopción en el mercado ha sido muy reciente y requiere que los proveedores garanticen su disponibilidad en las actualizaciones de software y firmware.

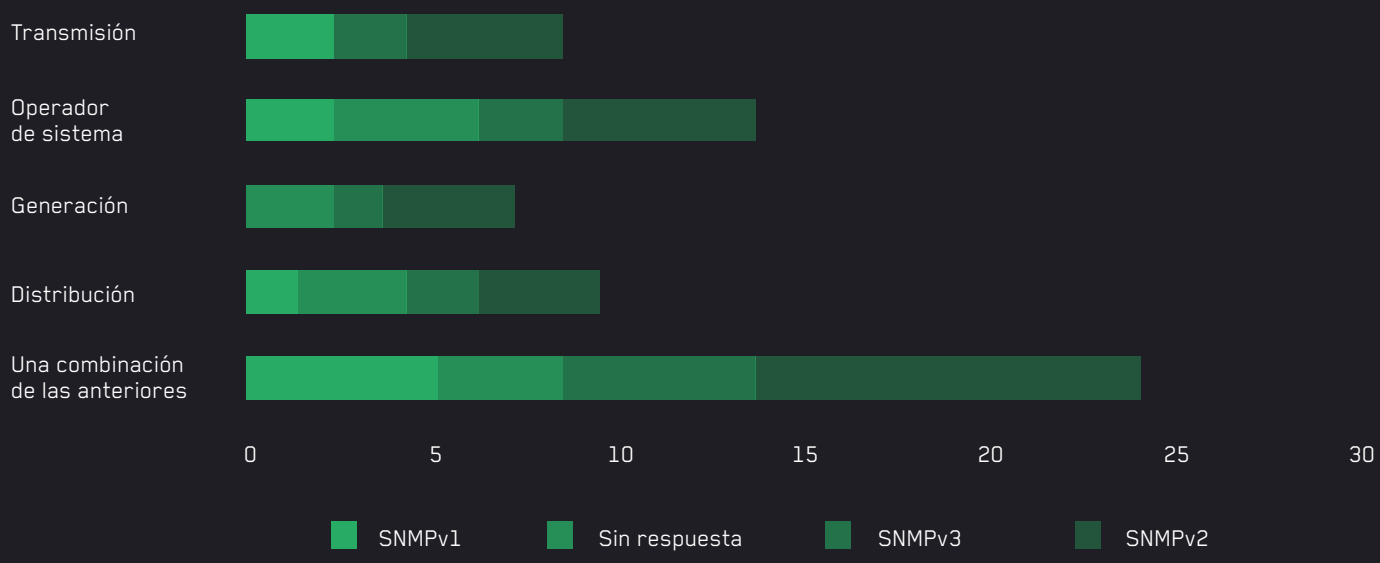


FIGURA 29. Uso del protocolo SNMP

En relación con el uso de WiFi (IEEE 802.11) en las redes TO, es notorio que en todos los sectores hay empresas que tienen como política impedir la operación de dicho protocolo en su red TO (Ver Figura 30). Llama la atención que excepto en distribución, al menos una empresa por segmento cuenta con dispositivos que se autentican usando el reciente protocolo WPA3. Dos empresas del segmento combinado reconocen que usan WEP o nula autenticación en su red WiFI.

La necesidad de contar con el protocolo 802.11x disponible en las redes TO debe responder a un análisis del riesgo muy riguroso. Mas allá de implementaciones de protocolos de campo inalámbricos como puede ser la nueva versión de HART, es importante considerar que protocolos de servicio comunes en redes TI no estén disponibles en las redes TO.

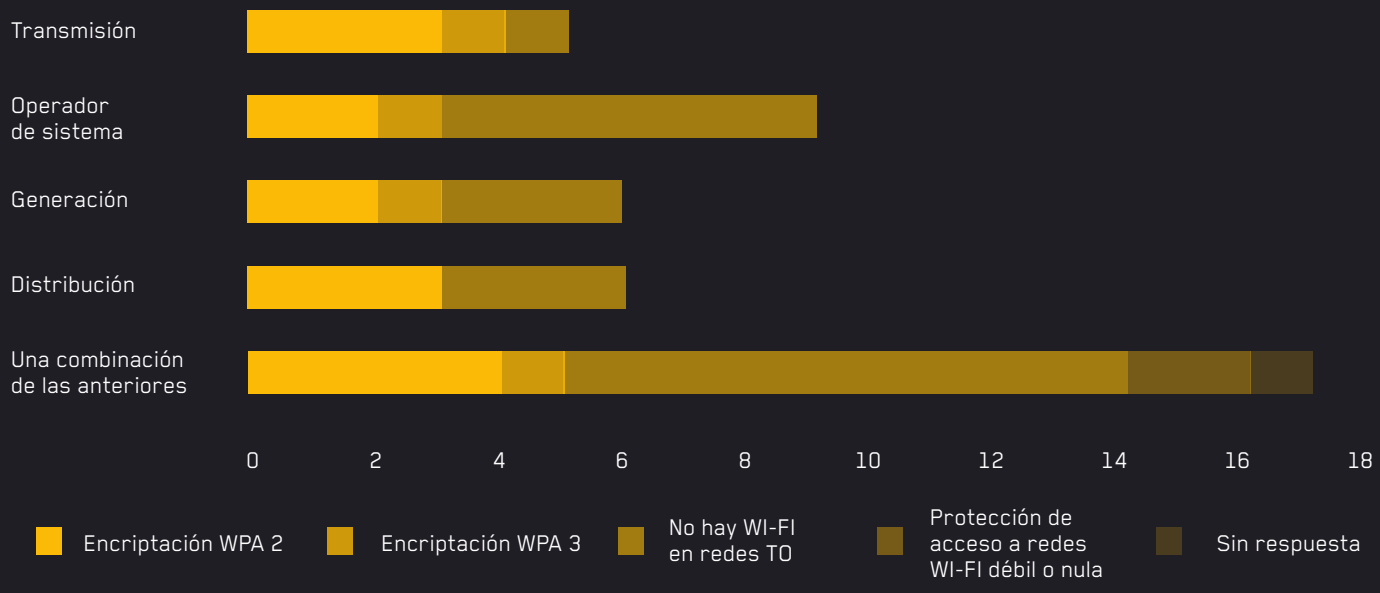


FIGURA 30. Uso de WiFi en redes TO.

3.4.6 | Gestión de la seguridad lógica

PREGUNTAS ORIENTADORAS

- ¿Su **organización** está utilizando **Firewalls (FW)** en su red operacional? (Figura 31)
- ¿El **enrutamiento del tráfico** de red entre las **VLAN** de su red **TO** está restringido por un **FW?** (Figuras 32 y 33)
- ¿El **FW** de su organización está **configurado** de acuerdo con la **política de seguridad** de su organización? (Figura 34)
- En su organización, ¿cuál de los siguientes **dispositivos** está protegido por **Endpoint Security (EPS)?** (Figura 35)
- ¿Cuál de las siguientes **opciones** describe las políticas de contraseñas de los **dispositivos de su organización?** (Figuras 36, 37 y 38)
- ¿Cuál es la **política de su organización** con respecto a las **contraseñas** de los **controladores lógicos programables** (Programmable Logic Controller o PLC)? (Figura 39)

¿Cuál de las siguientes **opciones** describe las **políticas de contraseñas** de las estaciones **ENG** de su organización? **(Figura 40)**

¿Cuál de las siguientes **opciones** describe las **políticas de contraseñas** de los servidores de **control de su organización? (Figura 41)**

¿Qué **controles de seguridad** utiliza su organización en el proceso de **fortalecimiento de los servidores** de control? **(Figuras 42, 43 y 44)**

¿Cómo **impide** su organización el **uso de medios extraíbles** no autorizados? **(Figura 45)**

¿Cuál es la **política de DLP** (Data Leak Protection) de su **organización? (Figura 46)**

Hoy día se disponen con los llamados Firewall de nueva generación NGFW (Next Generation Firewall) que son dispositivos que integran diferentes funciones, como por ejemplo la de enrutamiento de los paquetes de red. Estos dispositivos pueden estar en la capacidad de filtrar paquetes y protocolos propios de redes TO.

En los segmentos de transmisión generación y distribución hubo empresas que reconocieron que no contaban con firewall en sus redes TO (Ver Figura 31). En donde si está presente conviven tanto los que son industriales como los que son genéricos de TI.

Al indagar en cuales infraestructuras el tráfico es enrutado por el firewall o no, una empresa de transmisión y otra de operación indican que sus firewalls no realizan esta tarea (Ver Figura 32). Esto indica que cuentan con enrutadores dedicados y hacen que la carga del firewall solo sea dedicada al filtrado de los paquetes.

Organizaciones maduras consideran en su infraestructura que los equipos de misión crítica sean dedicados. Esto quiere decir que equipos del tipo NGFW no siempre sean los más adecuados para la gestión de todo el tráfico. De esta manera contar con enrutadores (routers) y conmutadores (switches) dedicados donde sea posible configurar QoS sobre los servicios críticos sea la mejor opción. En relación con el uso de firewalls, nuevamente, para ser usados en redes TO, en sus conductos y las interfaces con la red TI, deberían contar con perfil industrial, que les permita no solo reconocer los protocolos de campo, sino garantizar latencias mínimas en la red.

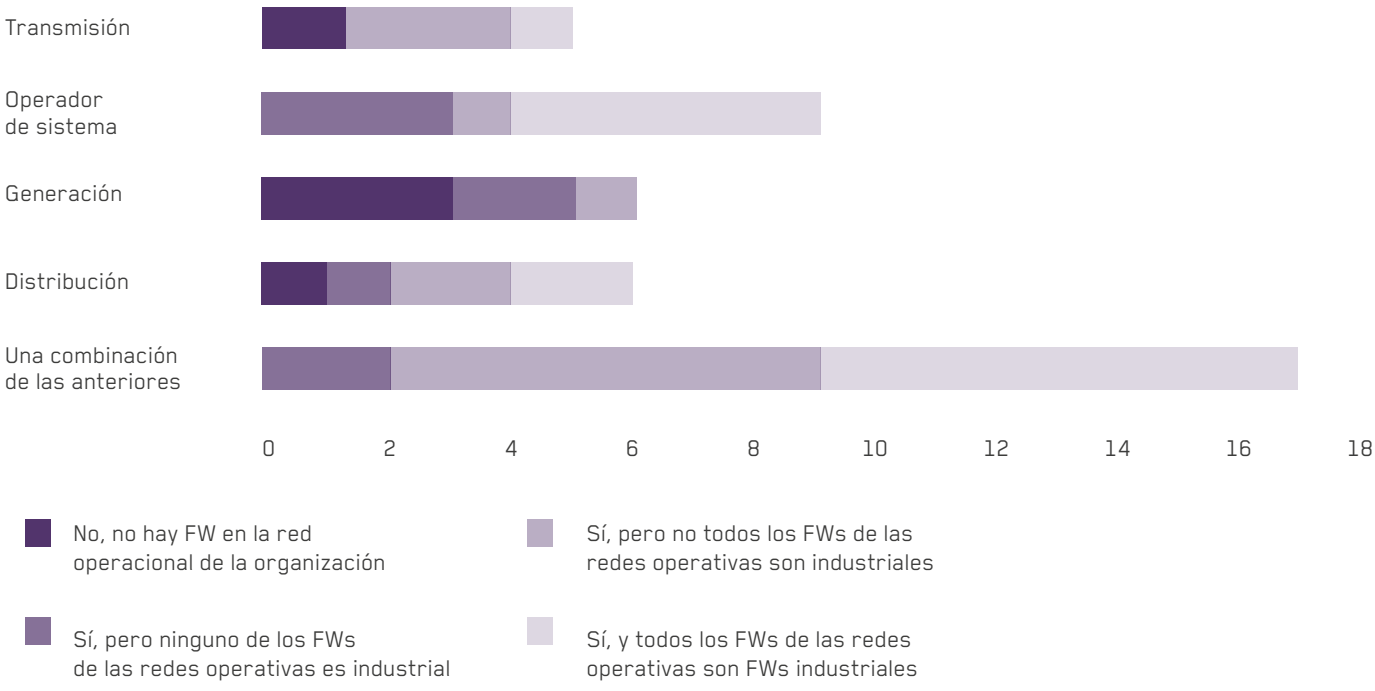


FIGURA 31. Uso de firewall en la red TO.

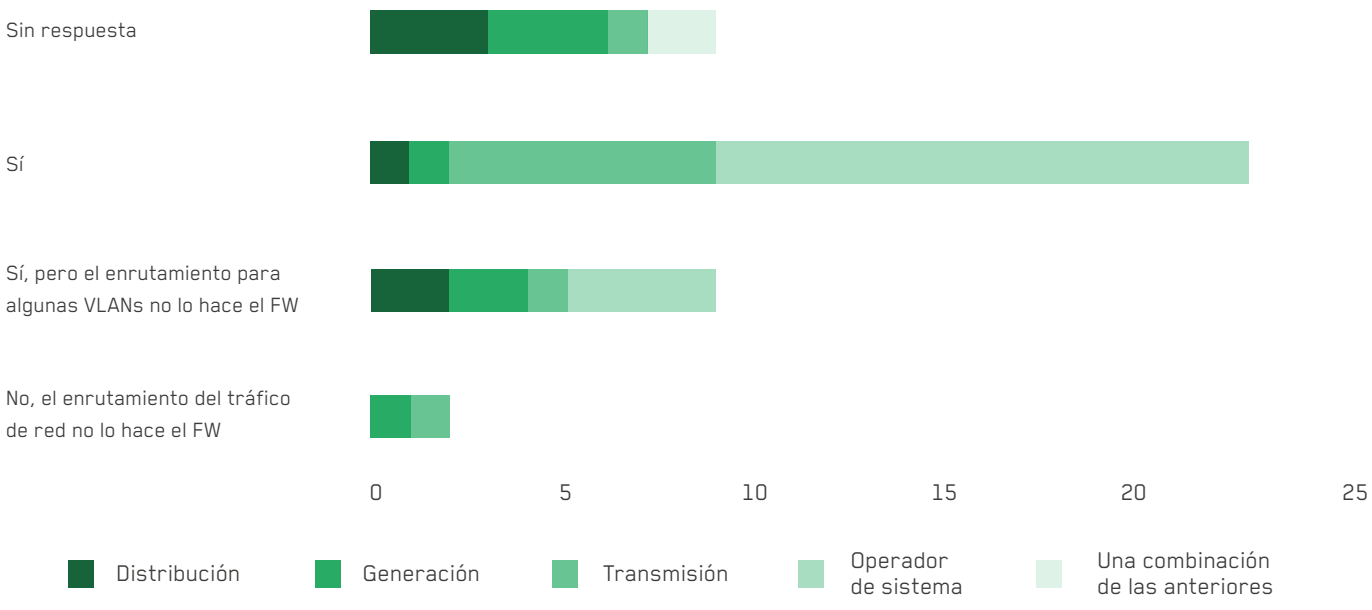


FIGURA 32. Enrutamiento del tráfico por el Firewall.

La efectividad del firewall está basada en la calidad de las reglas definidas. En la Figura 33 se observa que empresas de los diferentes segmentos han definido reglas para el filtrado de protocolos, solo dando el paso a los permitidos explícitamente. Llama la atención de una empresa que indica que su firewall no bloquea ni registra ningún protocolo específico.

Este aspecto guarda estrecha relación con lo evaluado en la cadena de suministro. Una adecuada configuración del filtrado de paquetes viene de un buen conocimiento de la infraestructura instalada, así como del conocimiento de las buenas prácticas del mercado relacionadas con los ambientes industriales. Evitar emplear únicamente las recomendaciones que suelen dar los fabricantes pensando en redes TI, y que se considere lo propio para TO.

Otro elemento importante para considerar es cómo estos dispositivos están conectados a plataformas de monitoreo tipo SIEM, que permita conocer el comportamiento de la red y definir las alertas en caso de detección de anomalías. Para ello, es crítica la configuración de los registros de eventos y sus niveles a ser reportados.

Los firewalls en las **redes TO** deben responder a **configuraciones específicas** que garanticen la disponibilidad.

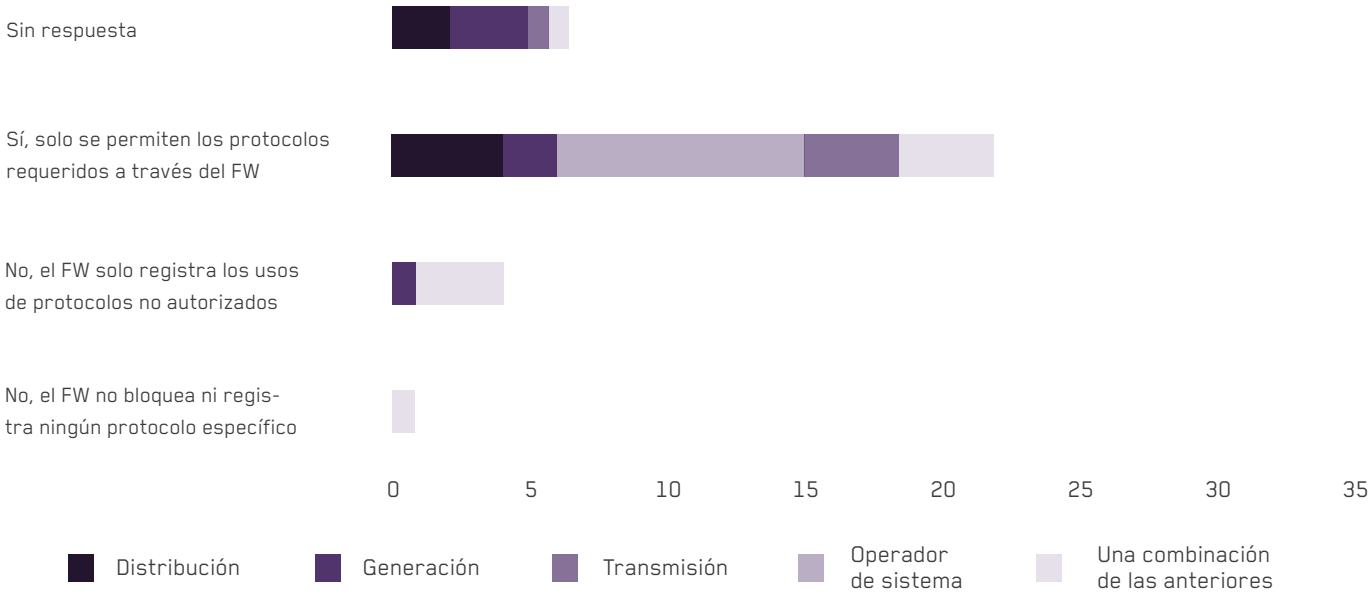


FIGURA 33. Reglas de filtrado de tráfico.

Los firewalls en las redes TO deben responder a configuraciones específicas que garanticen la disponibilidad. También allí se deben reflejar las reglas que derivan de las políticas de seguridad definidas por la alta gerencia. En la Figura 34 se describe quien ha configurado el firewall y si no responde a las políticas de seguridad TO. Se llama la atención que tres empresas reconocen que usan un proceso intuitivo de prueba y error para configurar el dispositivo. En los otros casos el firewall ha sido configurado siguiendo las buenas prácticas del mercado y respondiendo a las políticas de seguridad. No está generalizado que debe haber revisiones periódicas para la incorporación de nuevas reglas y ajustes por nuevas amenazas.

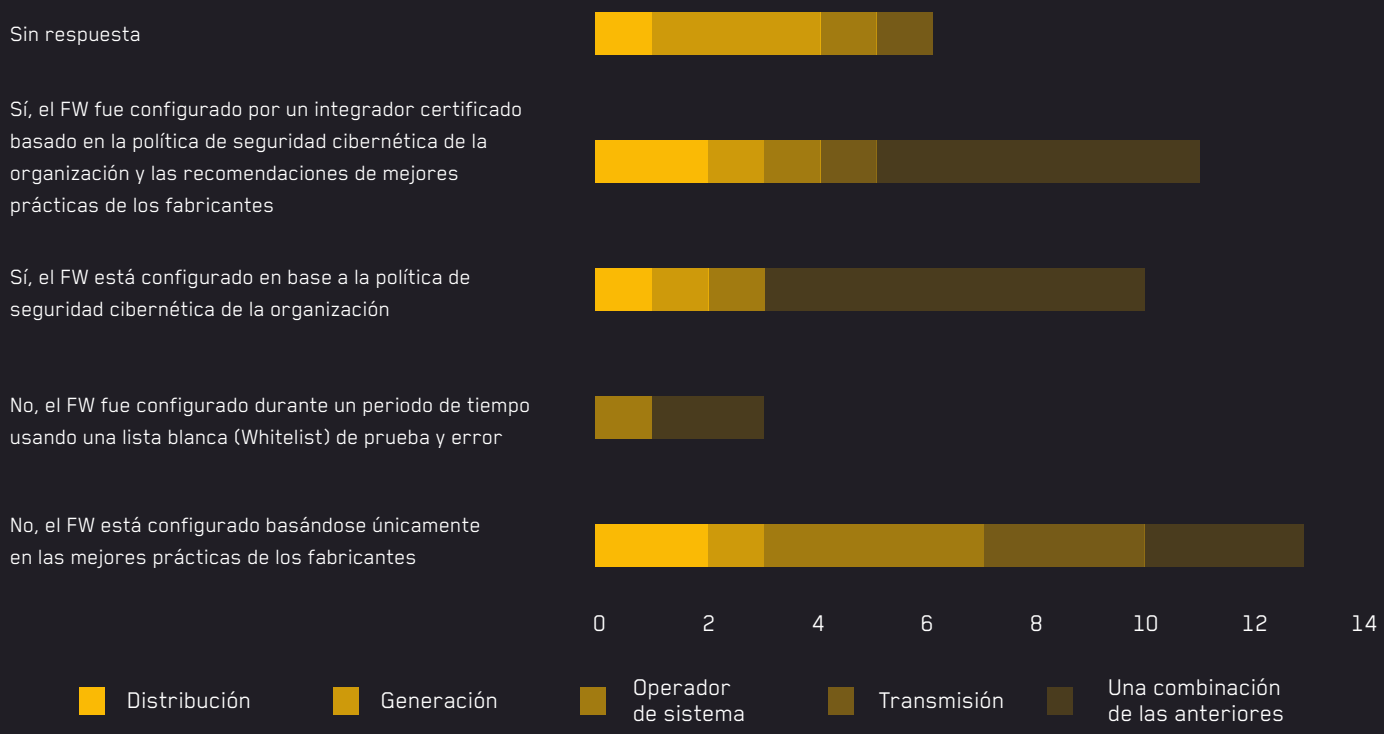


FIGURA 34. Política de configuración del firewall.

Se aprecia un consenso claro en la implementación de End Point Solutions para la protección de los diferentes equipos parte de la infraestructura TO (Ver Figura 35). Tan solo 10 empresas manifestaron que no cuentan con esta solución implementada.

Aunque es un punto de constante conflicto entre los responsables de TI y los de TO, la necesidad de proteger los equipos terminales es crítico. No solo los equipos de ingeniería, sino cubrir la mayor superficie de equipos que puedan ser sujetos de protección. El principio de seguridad por capas, estima que cada componente debe contar con la capacidad de protegerse a sí mismo, es por ello que es necesario contar con EPS en la red TO.

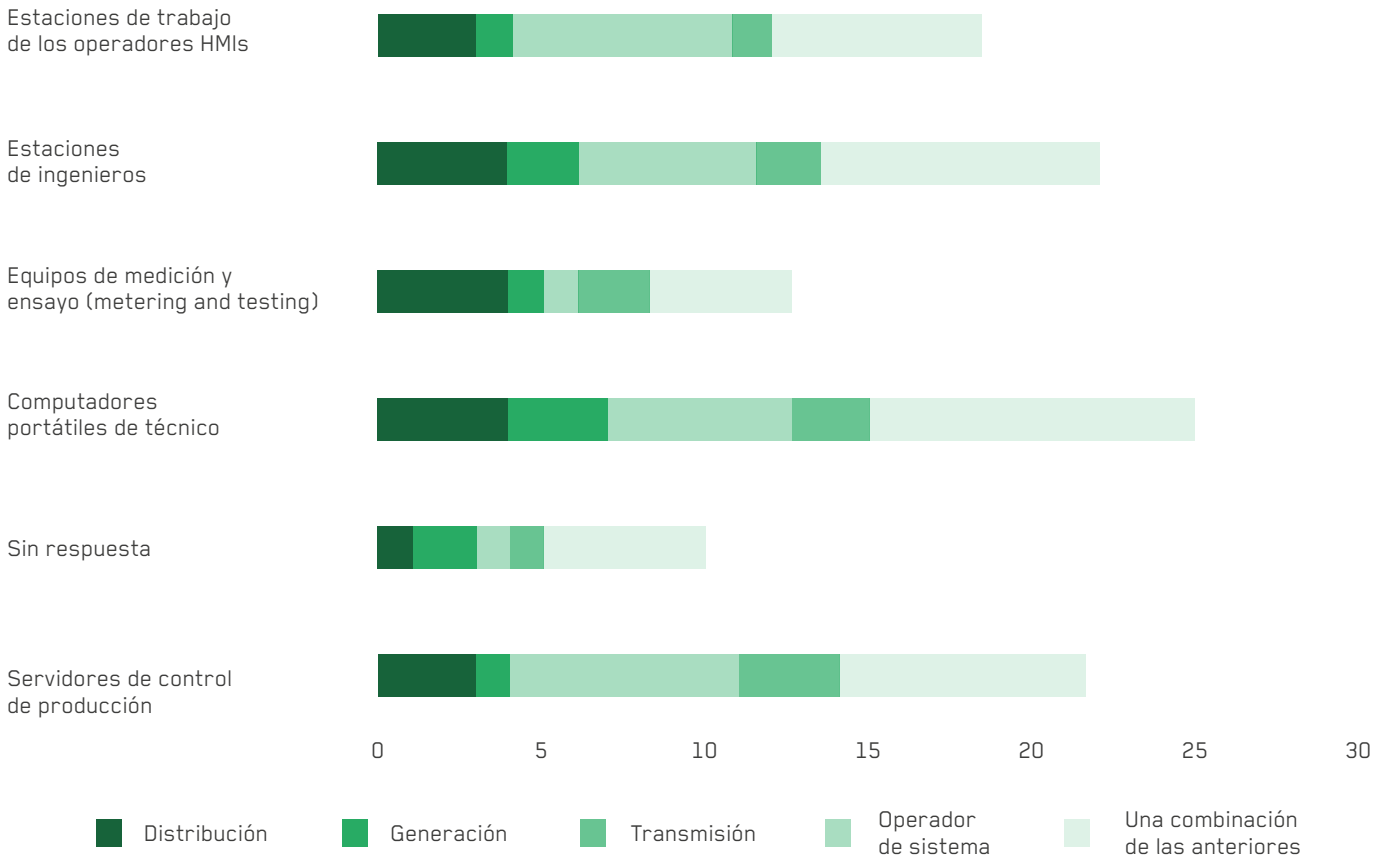


FIGURA 35. Equipos protegidos con EPS.

En la Figura 36 se aprecia como las empresas en todos los sectores reconocen que no cuentan con control de acceso de red en su infraestructura TO. De manera particular en el segmento de generación, ninguna empresa lo tiene instalado.

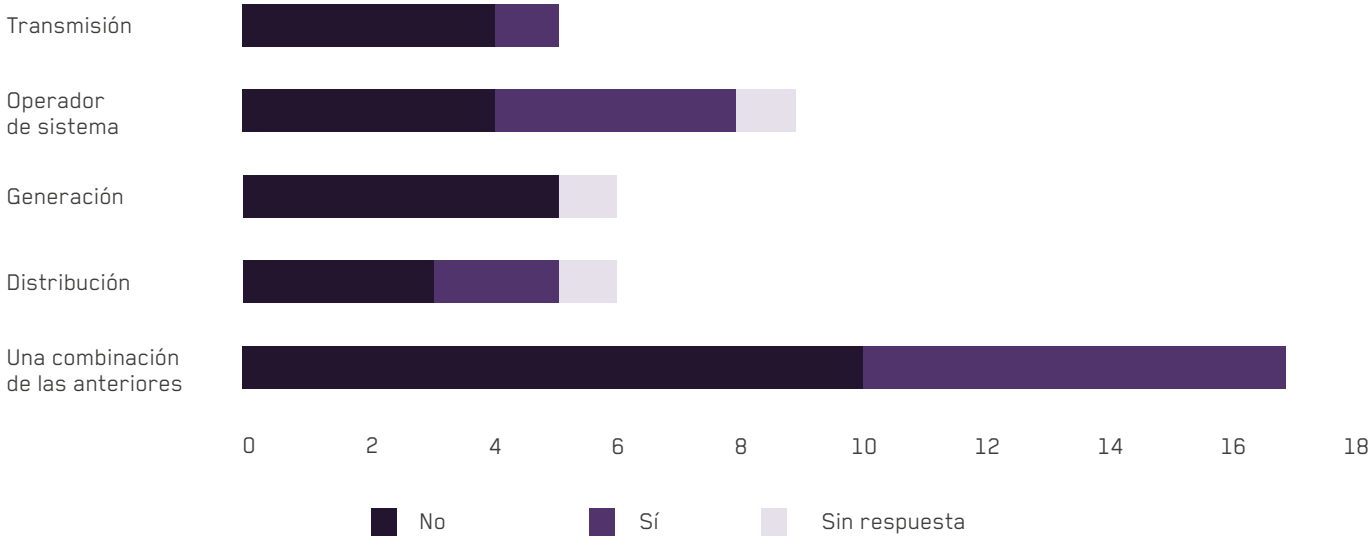


FIGURA 36. Control de acceso para TO.

La definición de una política para la gestión de acceso a los recursos y segmentos de red es descrita en la Figura 37. Tan solo dos empresas del segmento de generación indican que su política no limita el acceso y que todos tienen los mismos privilegios de acceso. Las demás empresas indican que cuentan con políticas más restrictivas que van desde la gestión individual de los usuarios, hasta la gestión de perfiles desde un directorio activo.

Tener una política de acceso a los recursos de la red TO se debe reflejar en las reglas que son configuradas en los equipos de protección y gestión. Una buena política describe la necesidad de segmentar las redes, definiendo el uso para cada VLAN. También describe el tráfico entre segmentos, la necesidad de conectarse con LAN, WAN e internet y uso de protocolos como el 802.11.

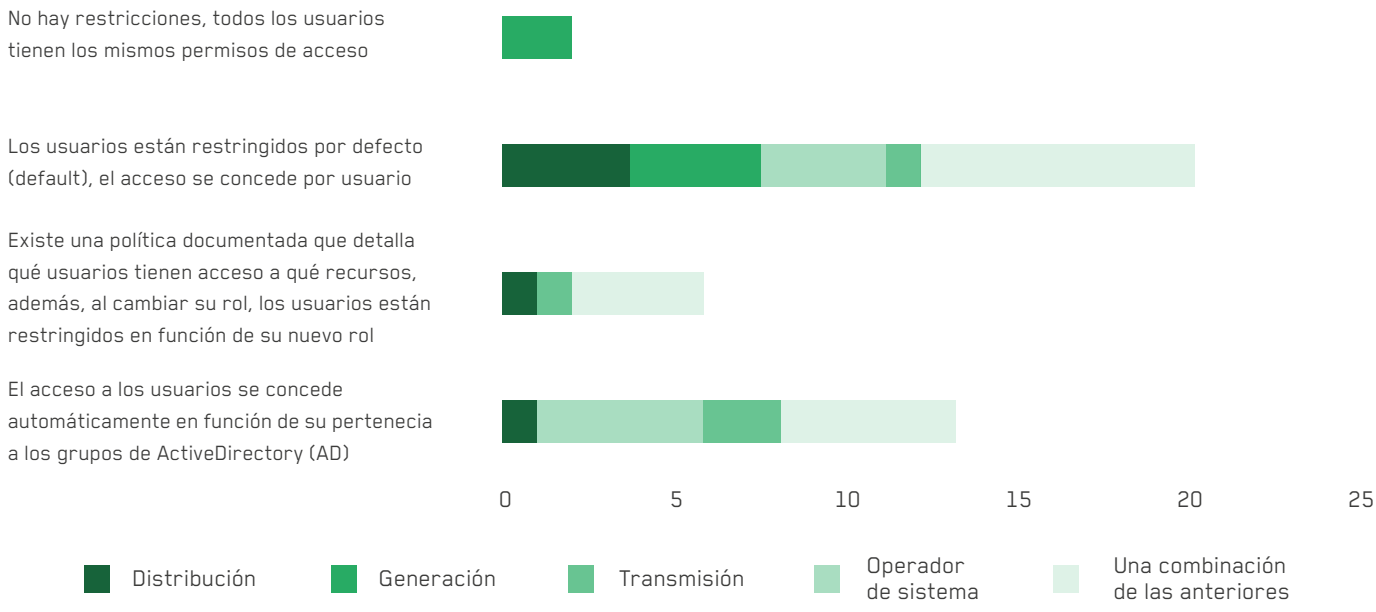


FIGURA 37. Política de acceso a los recursos de red.

A continuación, se describirá el manejo de las contraseñas que se está dando a los diferentes dispositivos en la red TO. Inicialmente se describe la política de contraseñas para los dispositivos de red (Ver Figura 38). Nueve empresas no contestaron a la pregunta, lo que puede indicar que no tienen política alguna definida. Se puede interpretar que la elección de compartir la misma contraseña para algunos de los dispositivos de red es una práctica usual. Sin importar si esta es robusta, el riesgo que encierra es que conociendo una contraseña se puede acceder a múltiples dispositivos de la red TO.

Las gestión de contraseñas en los PLC, las estaciones de ingeniería y los servidores de control, puede apreciarse en la Figura 39, la Figura 40, y en la Figura 41 respectivamente. Para los PLC y las estaciones de ingeniería se aprecia como empresas de generación, transmisión y multisegmento han indicado que tienen dispositivos sin contraseña alguna. Esto indica que no requiere ningún tipo de autenticación para acceder al equipo.

Otro elemento común para los tres tipos de dispositivos es que aún están configuradas las contraseñas por

defecto de los fabricantes. Esto le da una ruta directa para que un atacante pueda realizar un ataque sencillo de fuerza bruta y vulnerar dichos equipos. Nuevamente, el hecho que se compartan contraseñas entre los equipos de la misma clase implica que si se compromete la contraseña de uno de ellos, se compromete el acceso para el resto de los equipos.

Esto puede ser reflejo de la política tácita de seguridad por oscuridad: si el equipo no lo ve nadie, nada va a pasarle. Para evitarlo, es importante considerar este escenario a la hora de identificar los riesgos y valorarlo considerando que puede ser un cisne negro: un evento que tiene una baja probabilidad, pero con un alto impacto.

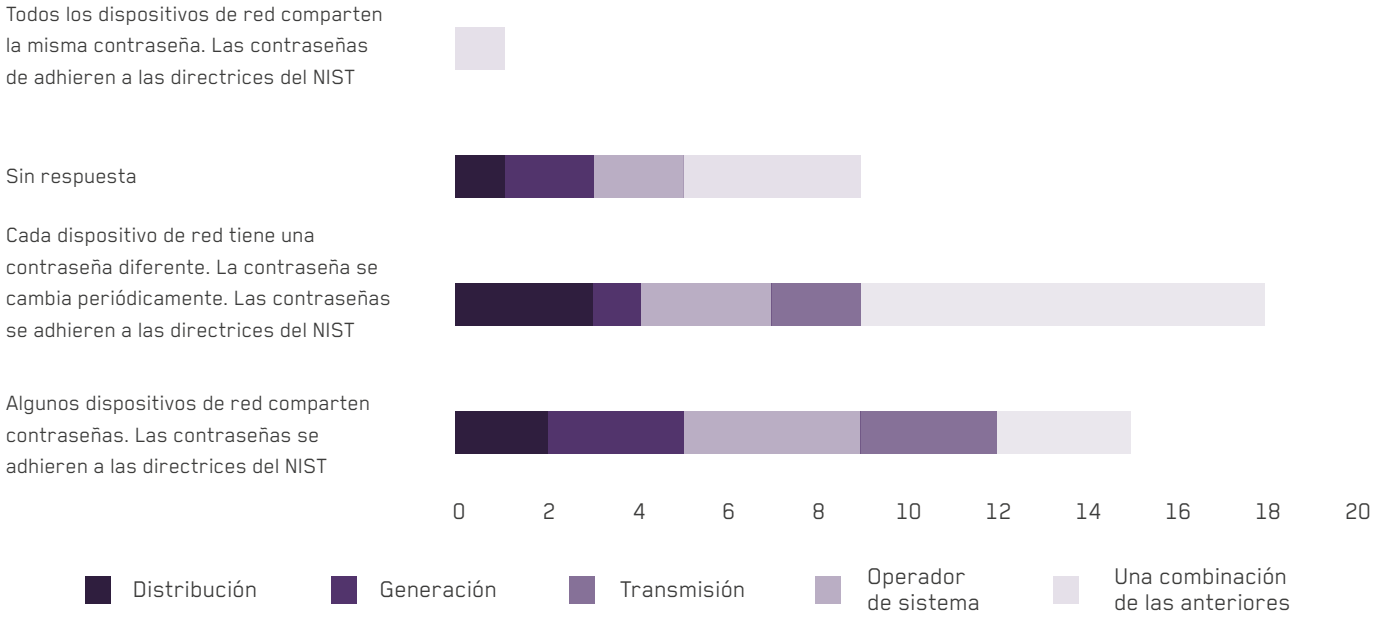


FIGURA 38. Política de contraeñas dispositivos de red.

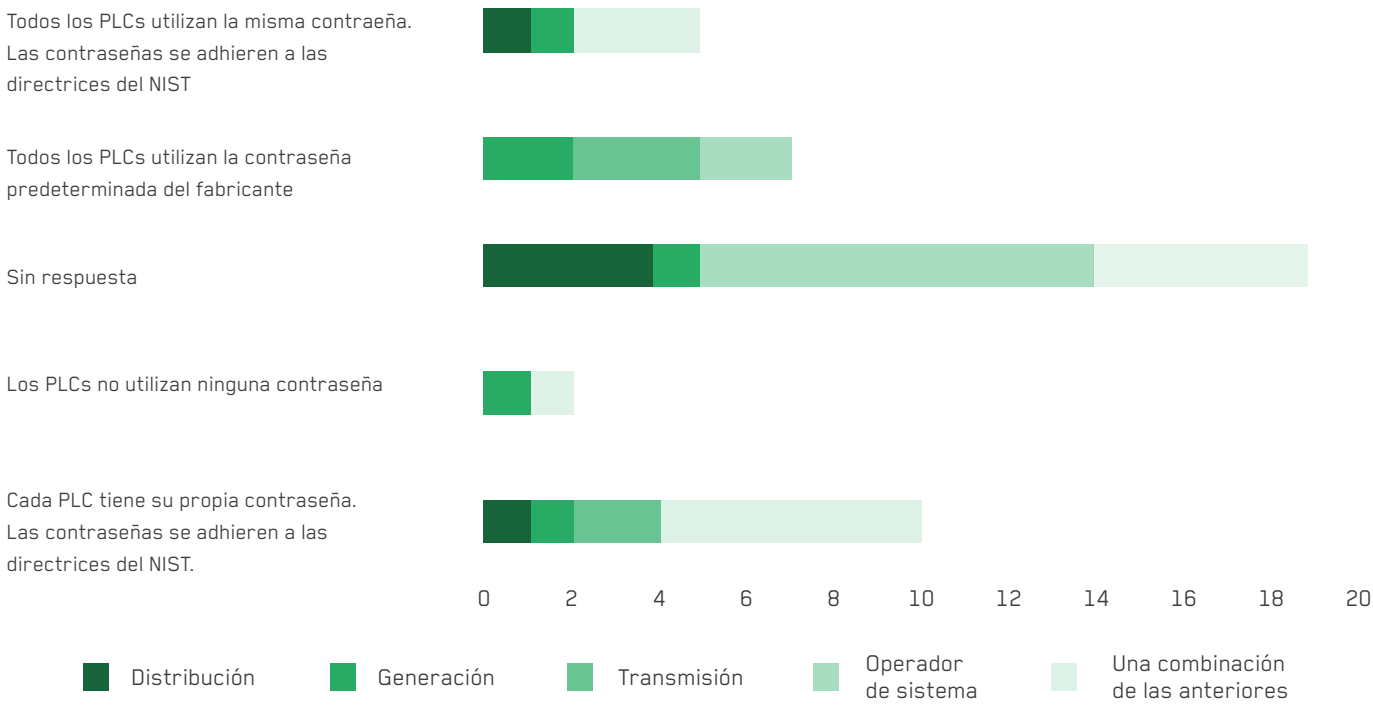


FIGURA 39. Uso contraseñas en PLC.

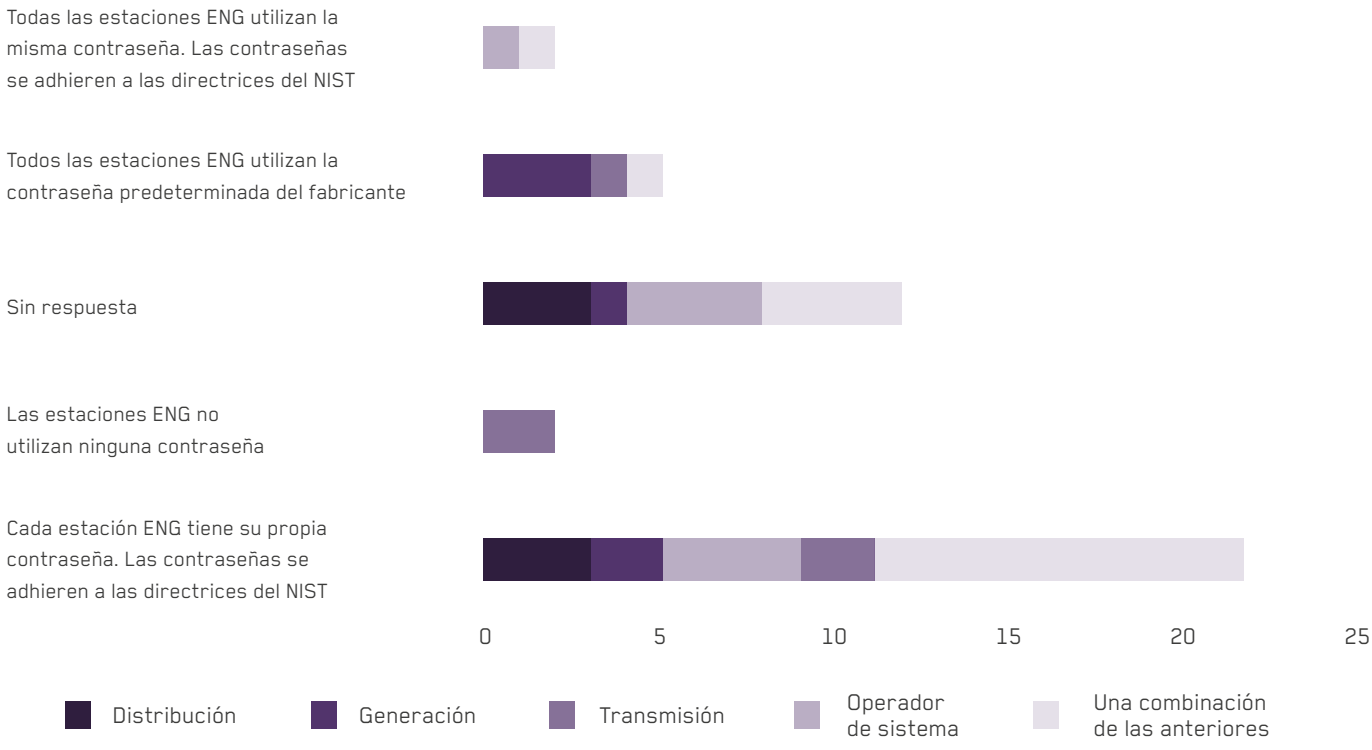
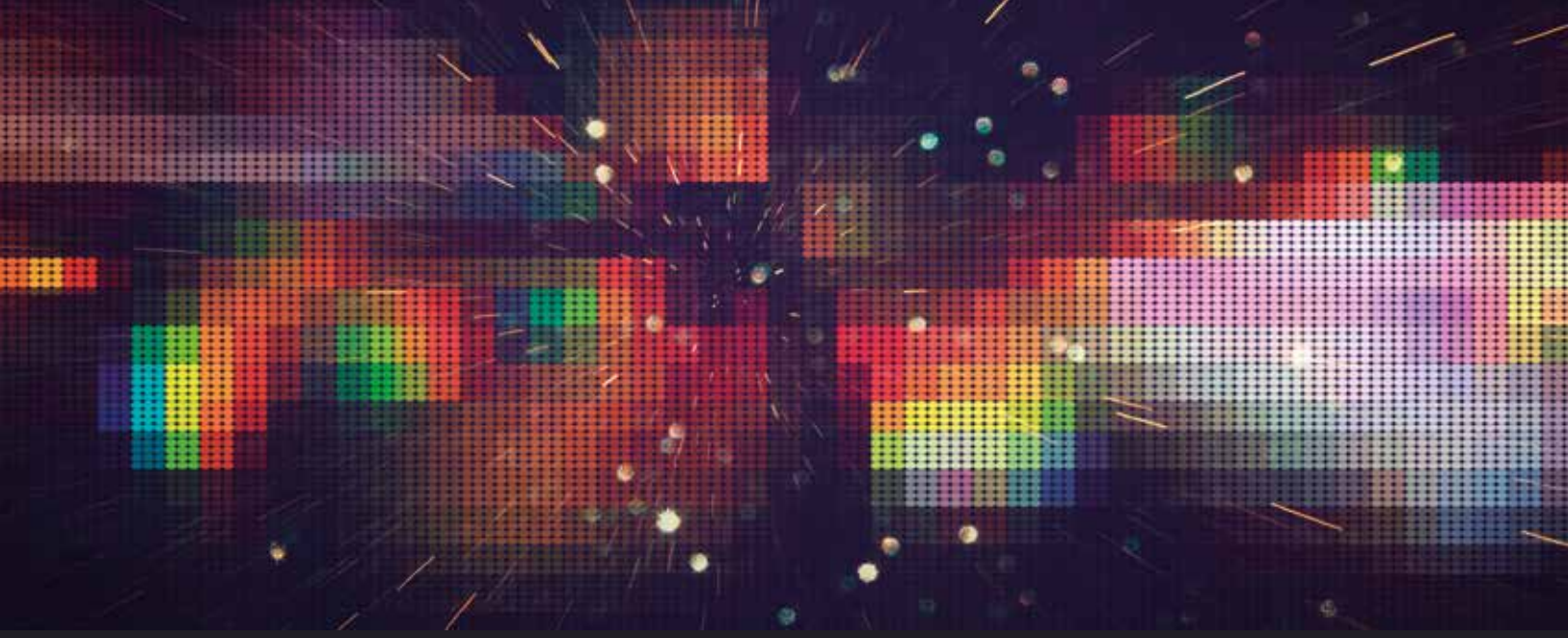


FIGURA 40. Gestión de contraseñas en las estaciones de ingeniería.



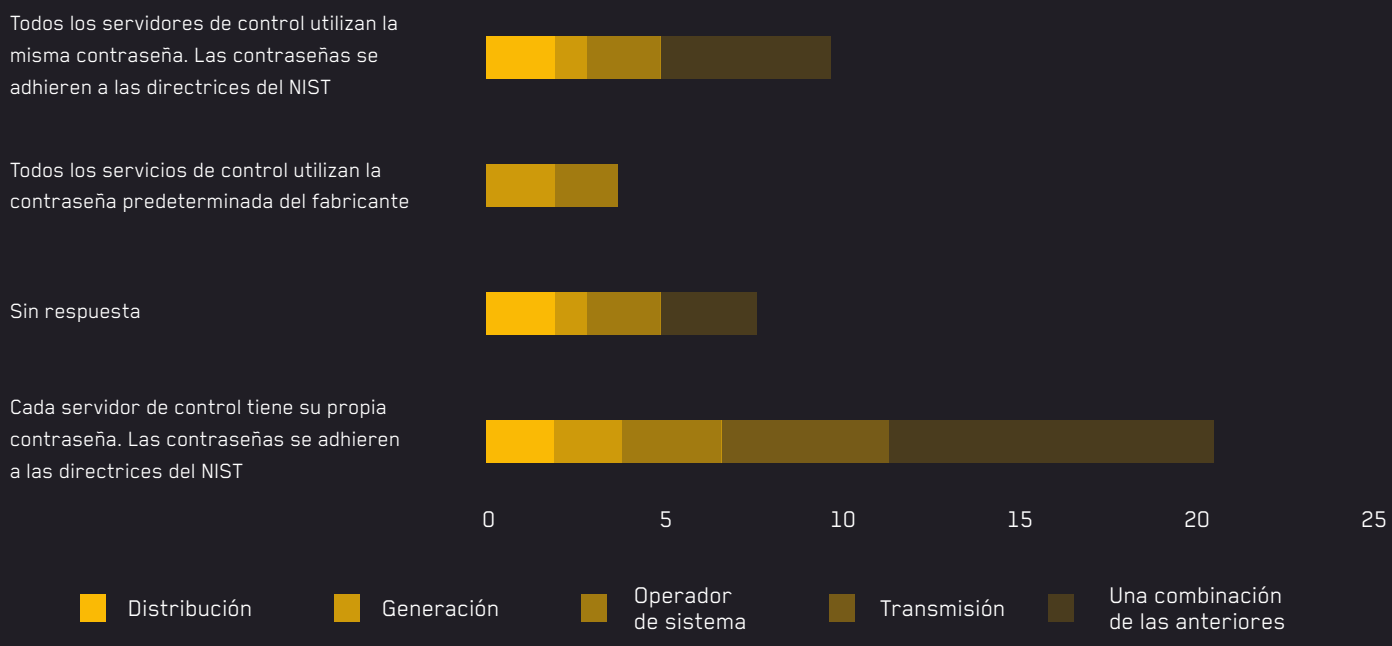


FIGURA 41. Gestión de contraseñas en los servidores de control.

Otro aspecto importante para considerar es la seguridad por capas. Esto implica que cada dispositivo debe estar en la capacidad de protegerse a sí mismo, y que cada conexión también sea protegida. Una de las aproximaciones para lograrlo consiste en bastionar los equipos. Aquí, cada tecnología va a contar con reglas y limitaciones específicas, incluso elementos de la misma clase, pero de fabricantes diferentes, puede enfrentarse a reglas de bastionado diferentes.

Para el bastionado de los PLC (ver Figura 42) se aprecia que las consideraciones mínimas a considerar no son seguidas por las empresas de todos los sectores. Algunas de ellas solo consideran un factor de autenticación como medida suficiente.

Establecer laboratorios de prueba, donde se verifique la operación de los PLC luego del bastionado, y que este responda a la política establecida se recomienda como buena práctica.

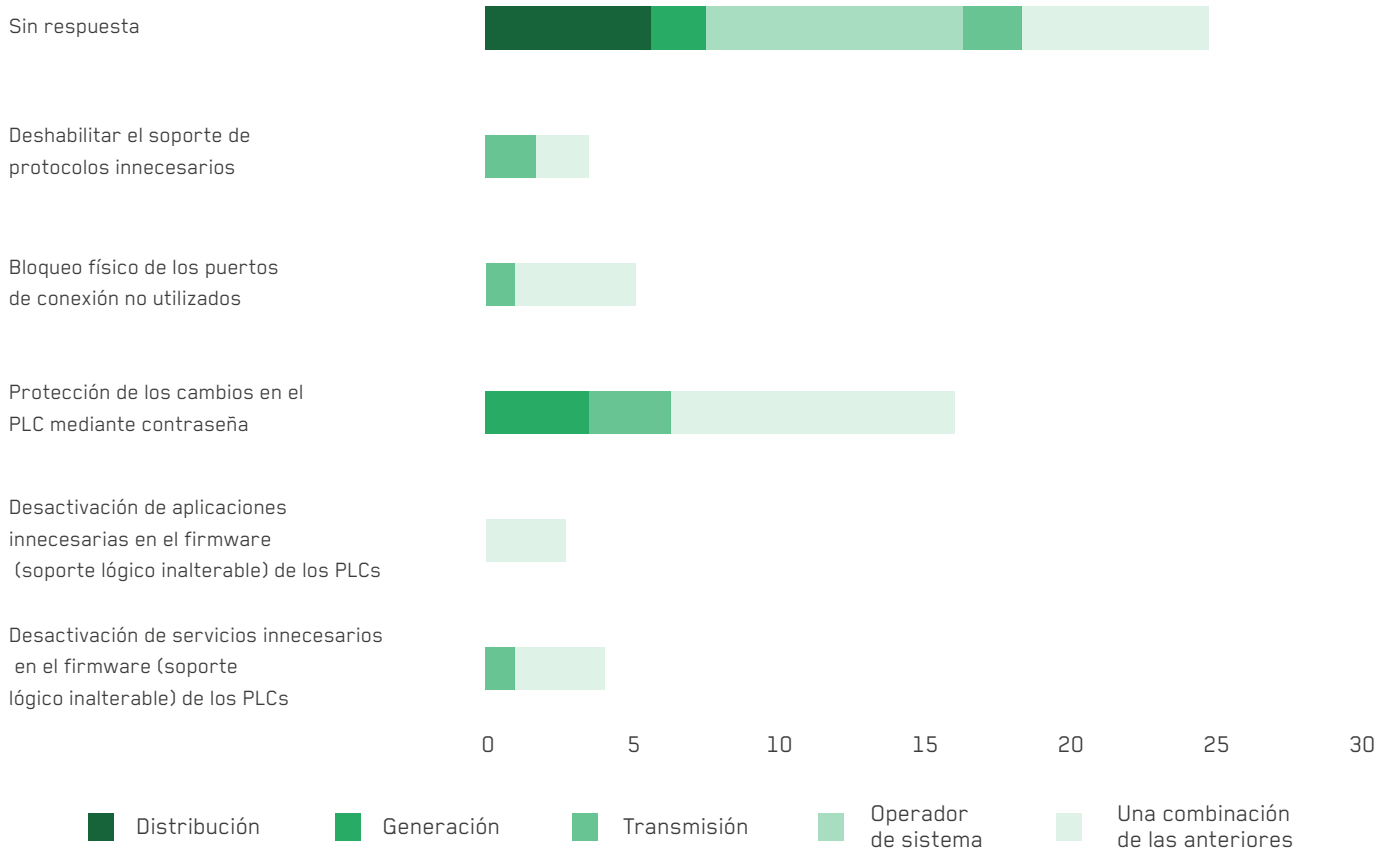


FIGURA 42. Bastionado de los PLC.

El bastionado de las estaciones de ingeniería (ver Figura 43) tiene mucha semejanza con las reglas establecidas para TI. Sin embargo, es importante considerar que en estos equipos van a estar instaladas aplicaciones de operación crítica en ambientes de alta disponibilidad.

Debido a su cercanía con las buenas prácticas de TI, es notorio como aquí se toman mas medidas para el bastionado. Sin embargo, las empresas del sector de la distribución no consideran todos los aspectos a proteger. Aunque las empresas de los demás sectores pueden implementar todas las recomendaciones, no es una constante y fallan en considerar todas las posibilidades.

Mientras que **25 empresas** expresaron que **no bastionaban sus PLC**, **12 manifestaron** que **no bastionaban** estaciones de **trabajo**

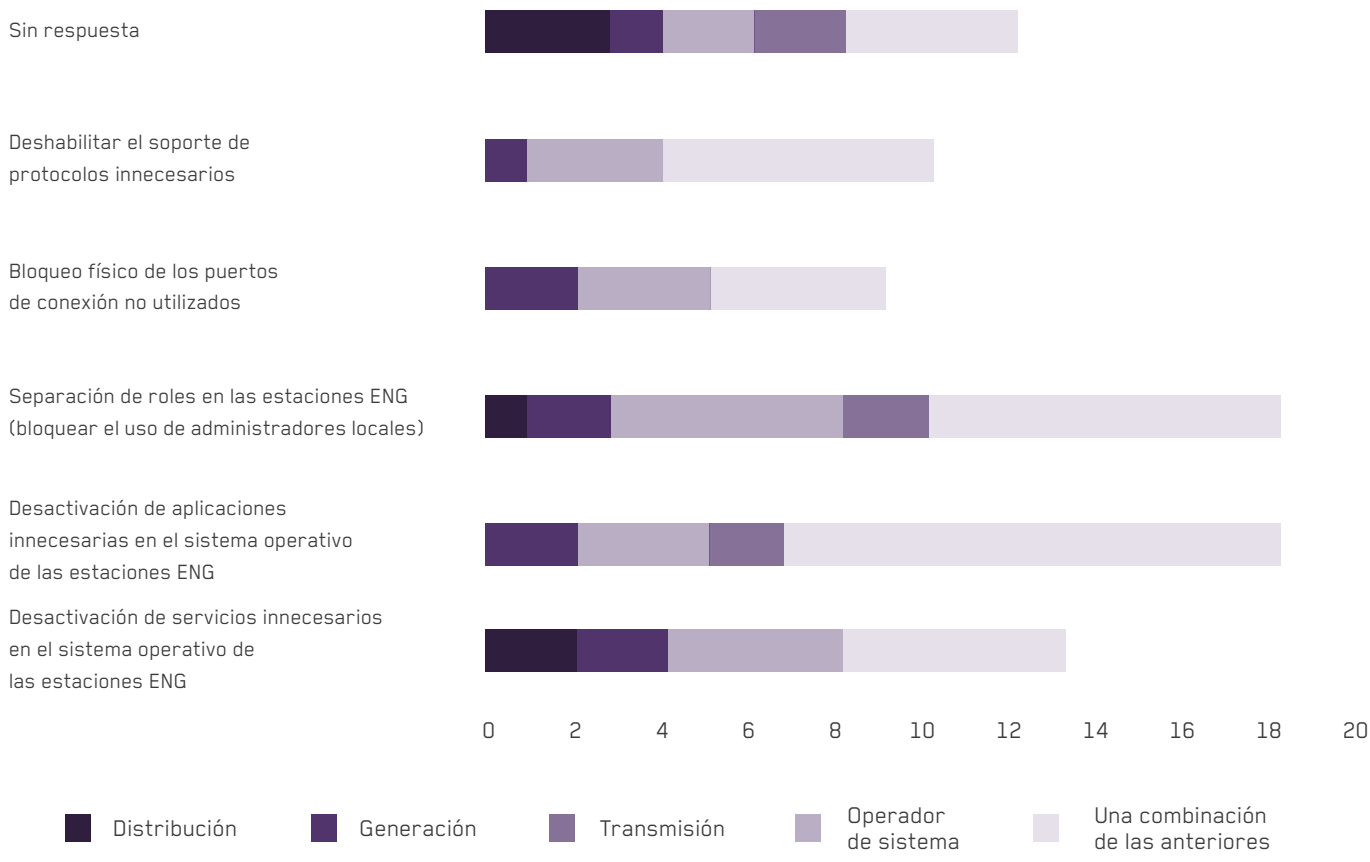


FIGURA 43. Bastionado de las estaciones de ingeniería.

Los servidores de control (ver Figura 44) comparten con las estaciones de ingeniería, que, al tener semejanzas con la infraestructura de TI, es más propensa a bastionarse de manera similar.

Sin embargo, se debe notar el comportamiento de quienes no implementan ninguna medida. Mientras que 25 empresas expresaron que no bastionaban sus PLC, 12 manifestaron que no bastionaban estaciones de trabajo, muestra que tan solo 8 indicaron que no bastionaban sus servidores de control.

En las que **sí bastionan**, se ve que **no siempre implementan** las **características** indagadas.

En las que sí bastionan, se ve que no siempre implementan las características indagadas. Aquí se recomienda tomar como base las plantillas de requerimientos mínimos que recomienda la industria y sobre ella construir el perfil que más se adecue a su infraestructura.

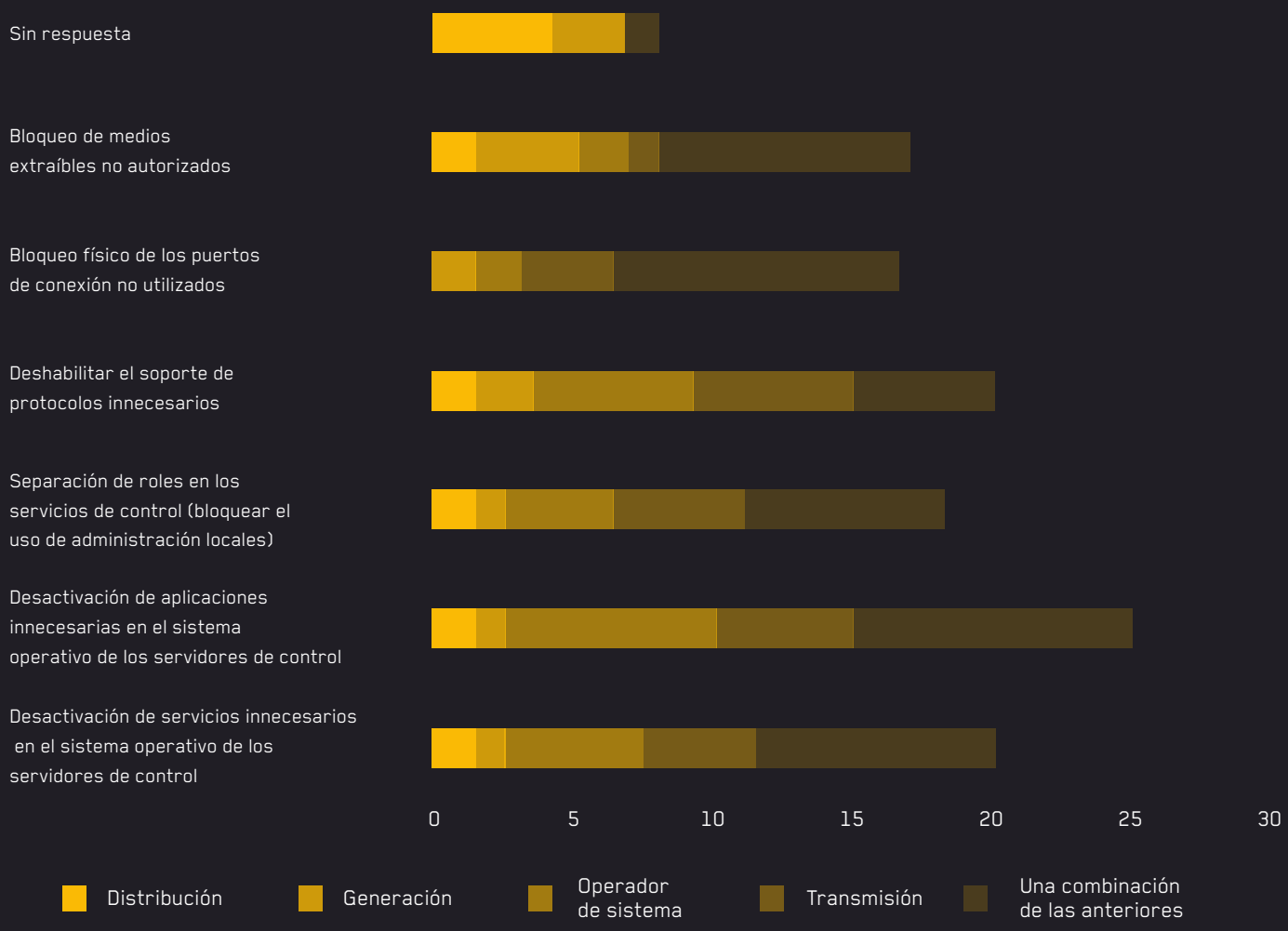


FIGURA 44. Bastionado de los servidores de control.

Cabe resaltar, que, aunque varias **empresas** manifestaron contar **con NGFW, ninguna** tiene implementado un **DLP** sobre este.

Para considerar los riesgos de las redes en la sombra (Shadow networks) que están relacionadas con los dispositivos extraíbles, se evalúa la política en la Figura 45. Aquí, 7 empresas indican que no cuentan con una política para dicha gestión. Cabe resaltar, que, aunque varias empresas manifestaron contar con NGFW, ninguna tiene implementado un DLP sobre este.

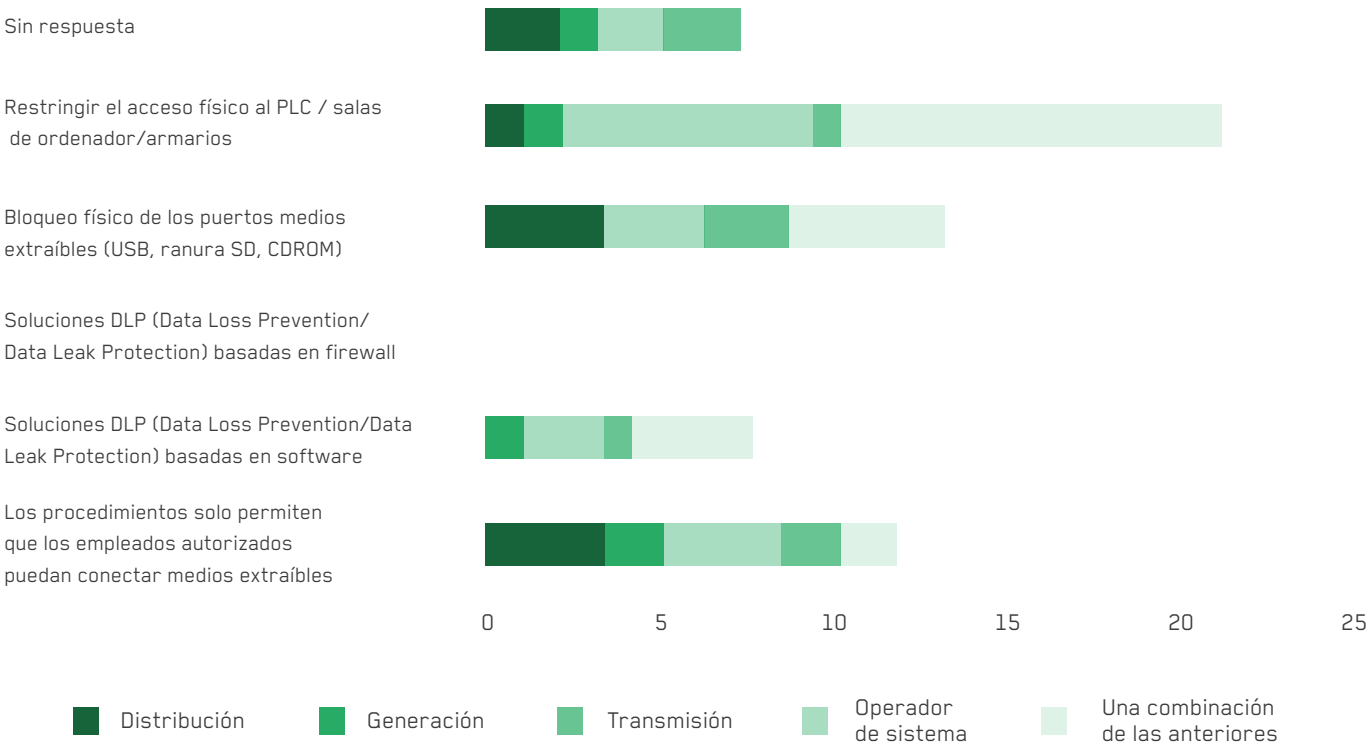


FIGURA 45. Política de medios extraíbles.

De las 7 empresas que indican que tienen una solución de DLP, solo 6 indican como lo gestionan (Ver Figura 46). No contar con una política activa en el DLP es reflejo que este está en modo aprendizaje, y no en operación. Tan solo dos empresas indican que tienen una política estricta configurada y monitorizada.

Se evidencia que aún las empresas no cuentan con la madurez suficiente para implementar un DLP. Esto no es negativo, siempre y cuando para los elementos básicos se garantice su implementación y correcto funcionamiento. Pero para aquellas empresas que si lo tienen implementado, es imperativo que pasen del modo de aprendizaje a uno más operativo donde tengan la capacidad de detección, y bloqueo y que se integre con los sistemas de monitoreo de la seguridad tipo SIEM.

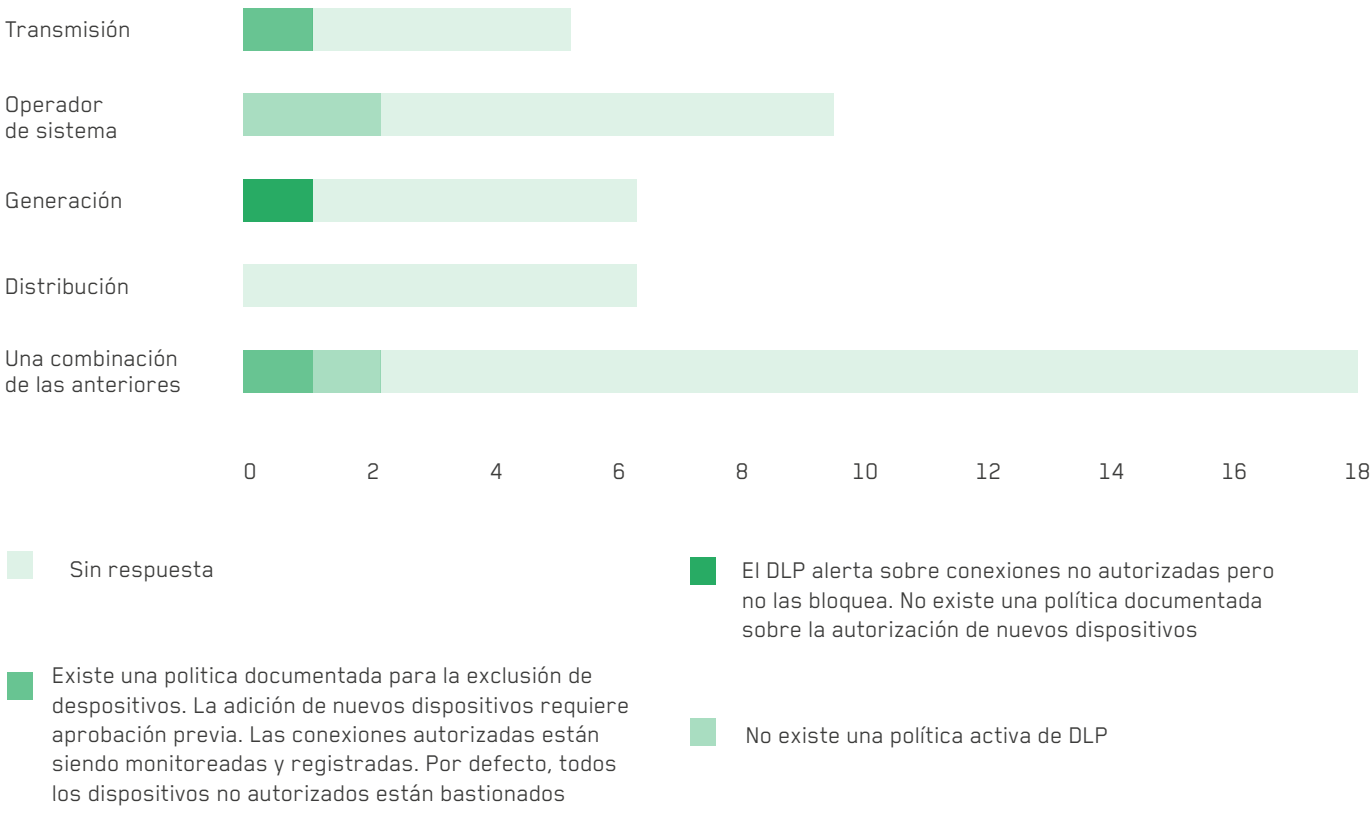


FIGURA 46. Política de DLP.

3.4.7 | Gobernanza de la seguridad

Es importante **considerar** que la **seguridad de la operación**, así como la **seguridad de la información** requiere un **gobierno**.

Es importante considerar que la seguridad de la operación, así como la seguridad de la información requiere un gobierno. Este debe ser liderado por la alta dirección de la organización (quienes deben contar con las competencias adecuadas) y reflejarse no solo en la documentación sino en la disposición de recursos humanos y materiales para garantizar su implementación.

3.4.7.1 | *Política general de seguridad*

La Figura 47 muestra algunos indicadores generales que reflejan el compromiso de la alta dirección. Unas seis empresas indicaron la ausencia de compromiso de la alta dirección.

Unas **seis empresas** indicaron la **ausencia de compromiso** de la alta dirección.

Esto refleja una realidad que suele presentarse al subestimar el impacto de la seguridad en la operación y sus acciones proactivas más que reactivas.

Otro aspecto que se detectó es el compromiso superficial, ya que si no se designa suficiente personal y se asigna presupuesto es muy poco lo que se puede realizar para garantizar una operación segura y gobernable.

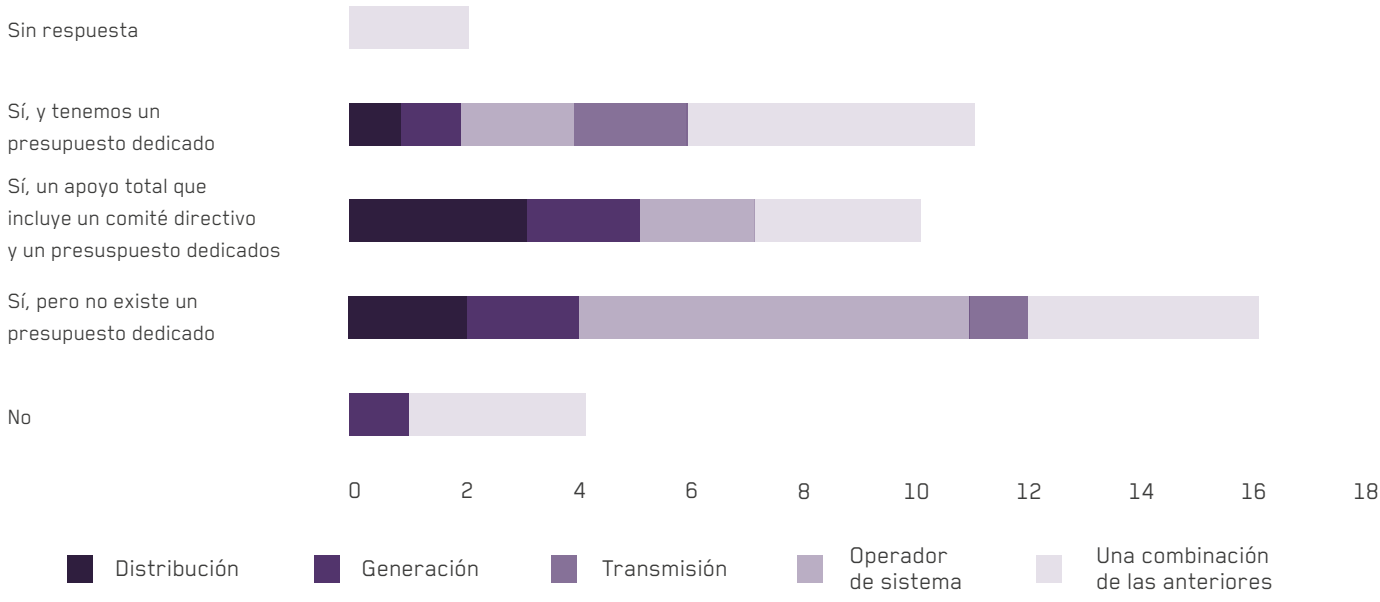


FIGURA 47. Compromiso de la alta dirección.

Uno de los elementos que reflejan el compromiso de la organización con la seguridad es la definición de una política específica para la seguridad en TO. En la Figura 48 se aprecia que 9 empresas no cuentan con una política, mientras que tan solo seis cuentan con una política completa definida. Siempre se habla del conflicto entre TI y TO, pero se evidencia que, sí existe una sinergia, puesto que 10 empresas de todos los segmentos han definido algunas referencias en su política de seguridad de la información para TI.

La política para que sea efectiva debe ser comunicada ampliamente a todos los miembros de la organización. Al menos 24 organizaciones indicaron que no comunican la política, mientras que el resto lo comunica por medio de mecanismos formales o informales.

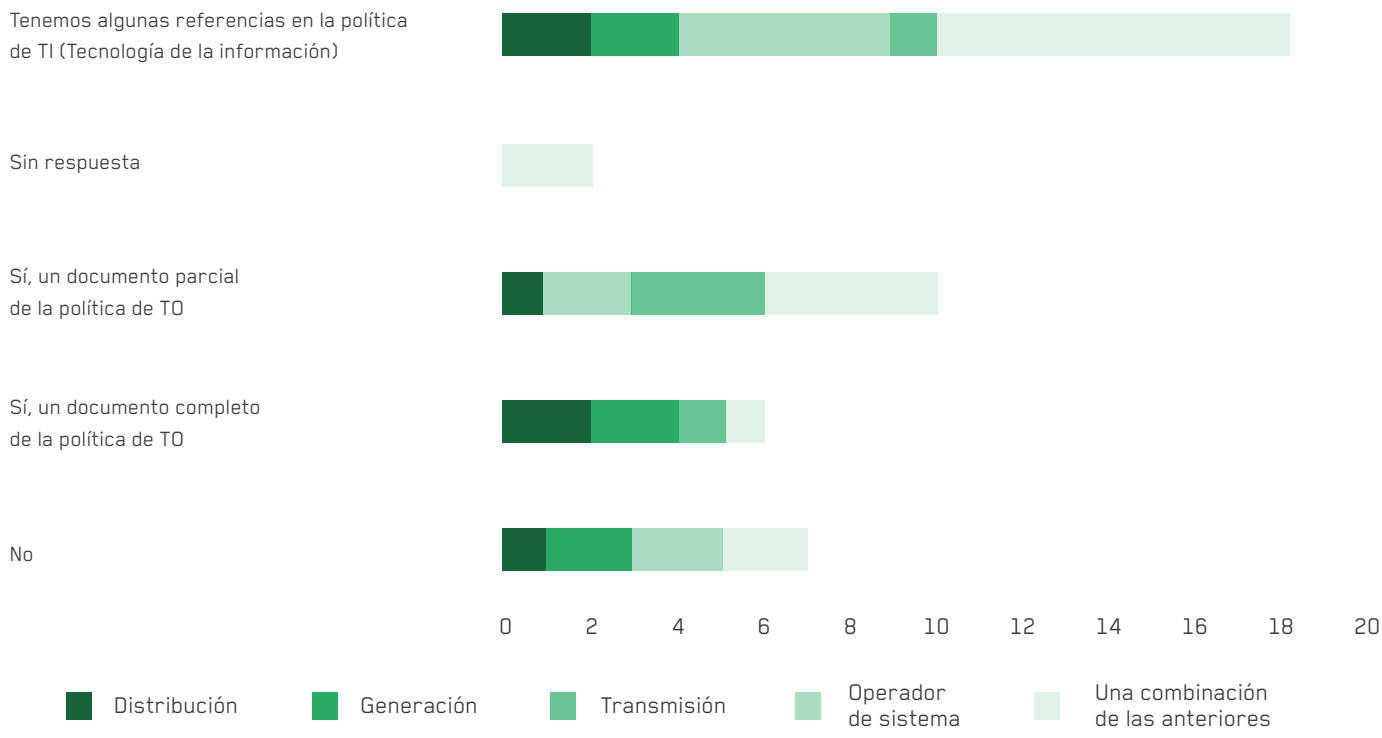


FIGURA 48. Política de seguridad para TO.

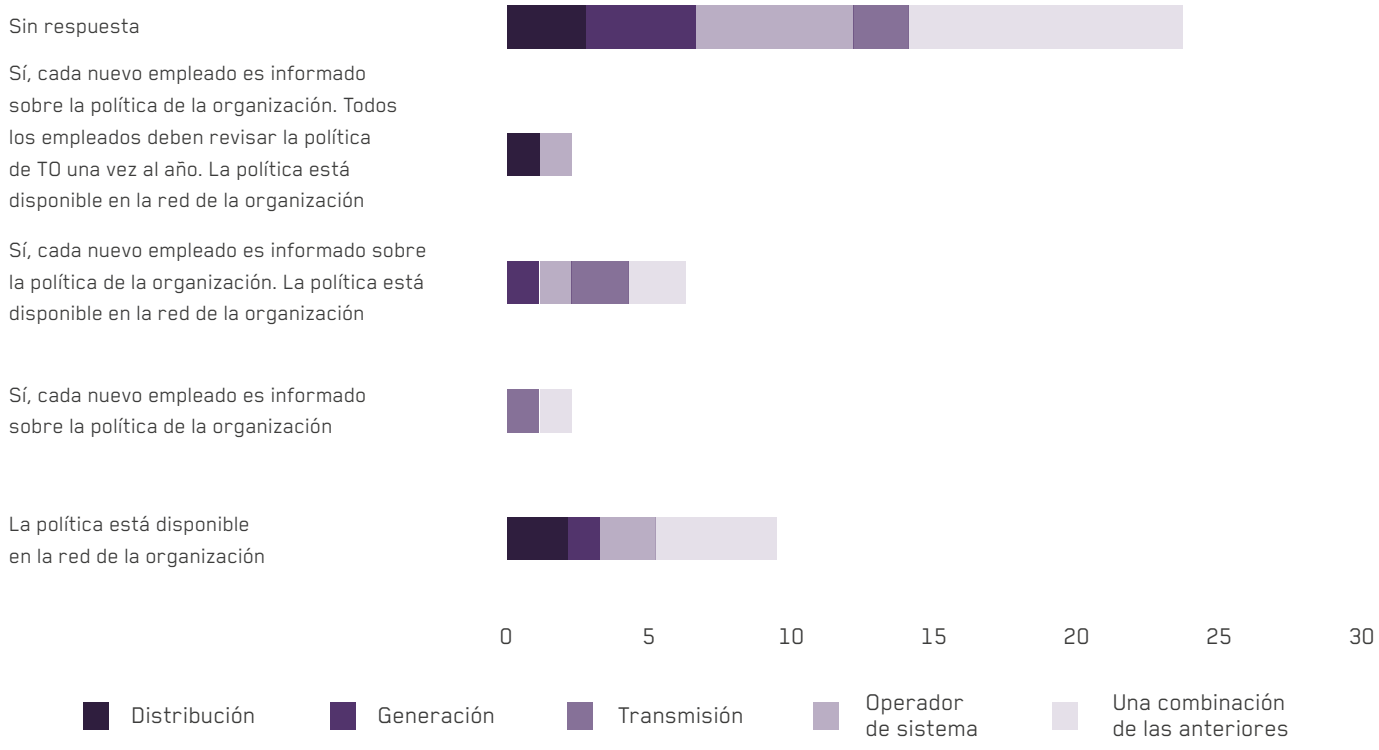


FIGURA 48. Publicación de la política de seguridad.

Cuando se revisa si la política definida tiene un proceso de revisión y actualización, 28 organizaciones indicaron que no hacen actualización alguna. Por otro lado, 8 de ellas realizaron su actualización hace más de un año. Esto refleja la ausencia de un sistema de gestión que garantice estos procesos como parte de la mejora continua. (Ver Figura 50)

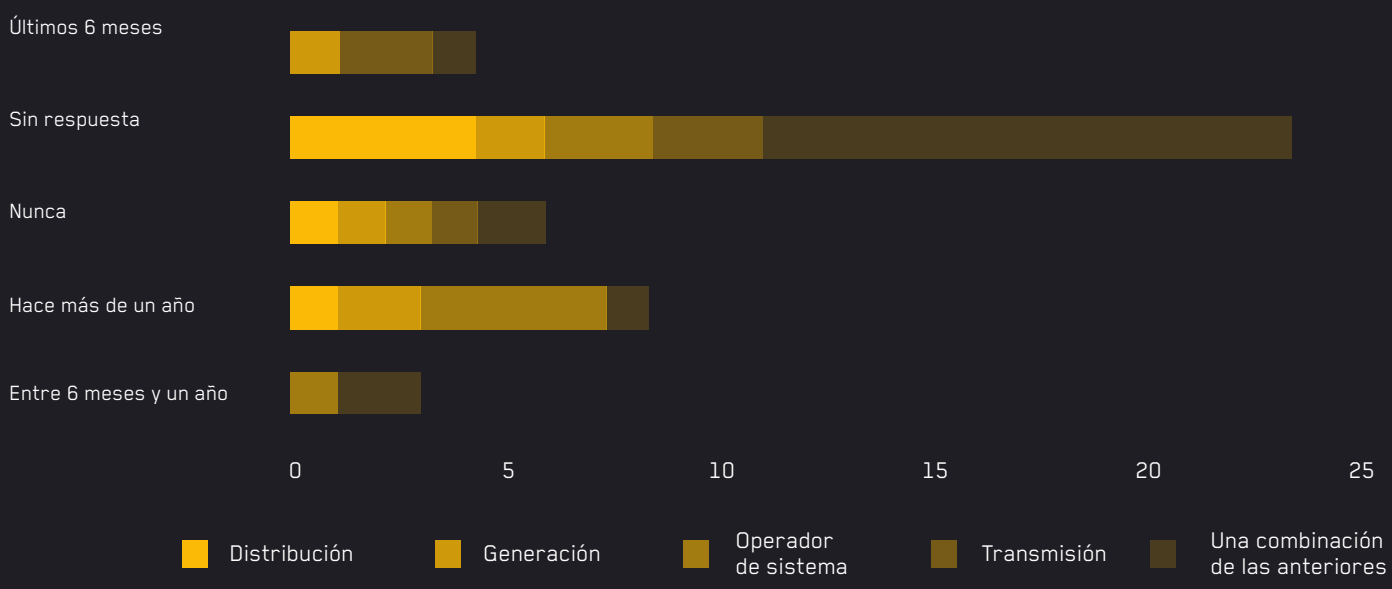


FIGURA 50. Actualización de la política.

La adhesión de la política a los diferentes marcos de buenas prácticas es indicada en la Figura 51, Figura 52 y Figura 53. Aquí se muestra que muy pocas organizaciones siguen estos marcos de buenas prácticas y se contradice con lo indicado en la Figura 48, puesto que, si una política es definida, esta ha de estar acorde con algún marco de referencia.

Contar con marcos de referencia permite establecer una línea base de buenas prácticas mínimas a implementar. Estas están para facilitar el camino y no depender de la intuición o el costoso camino de aprender cometiendo lo errores por los que otros ya pasaron.

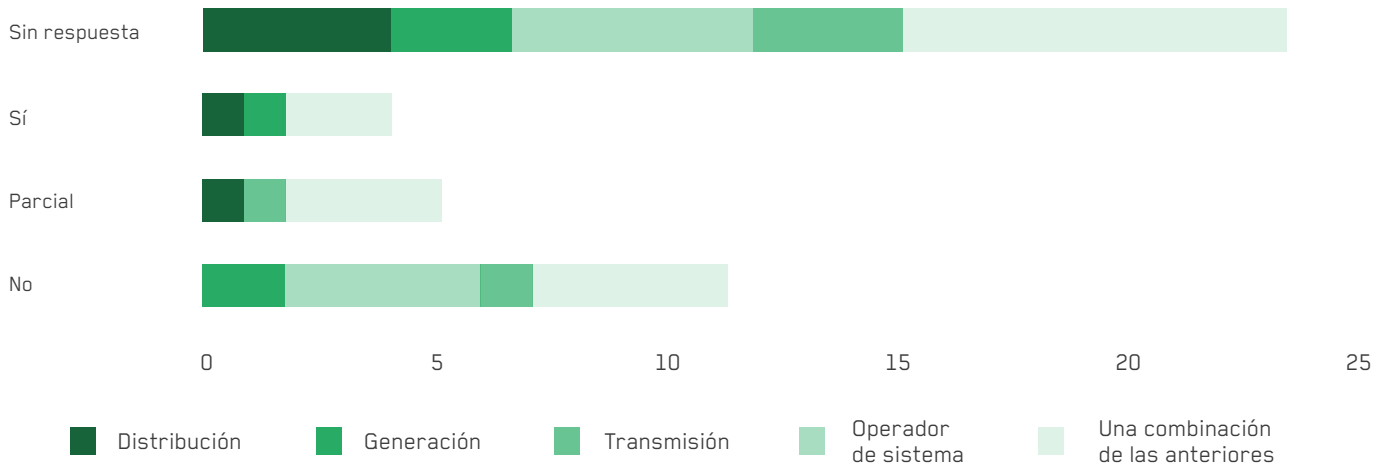


FIGURA 51. Compatibilidad con NERC.

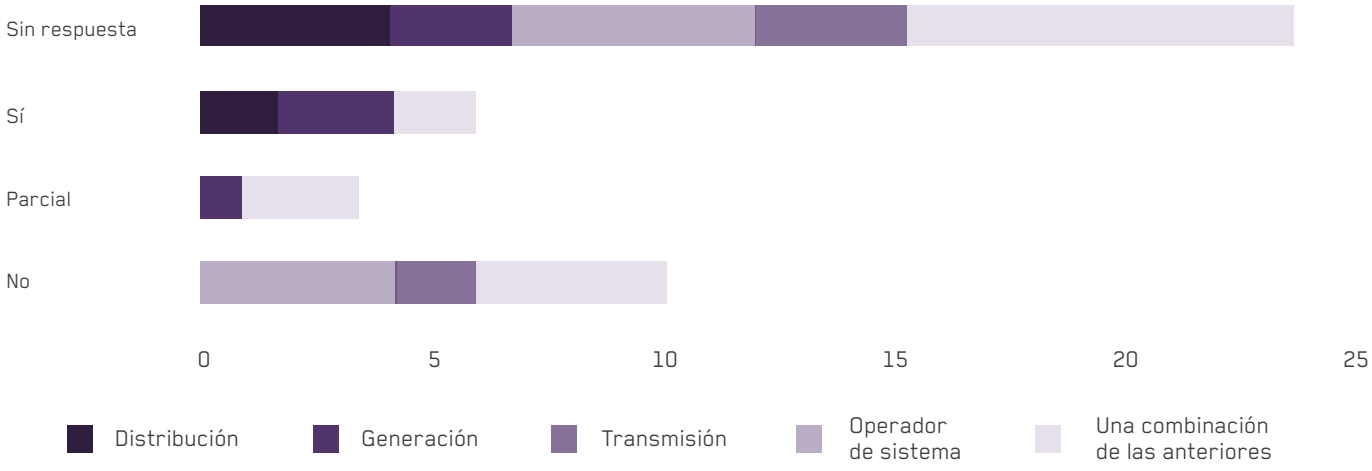


FIGURA 52. Compatibilidad con NIST.

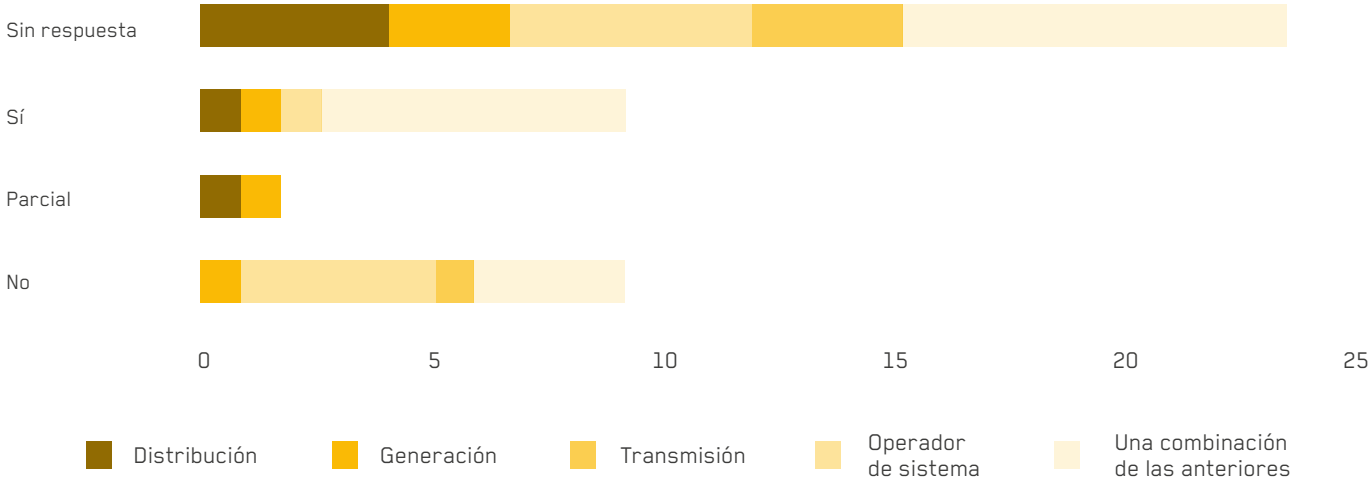


FIGURA 53. Compatibilidad con ISO/IEC 27001.

Todo sistema de gestión requiere contar con mecanismos que le permitan detectar sus desviaciones para así definir los planes de mejora. La auditoría es uno de esos mecanismos que permite cubrir toda la superficie o concentrar en solo algunos activos para verificar el cumplimiento de los controles definidos. Aunque hay empresas de cada segmento que no hace auditorías (ver Figura 54), es de resaltar que siendo la disponibilidad el principal pilar en la infraestructura TO, muy poco es auditado en el tema relacionado con la continuidad ante un ataque cibernético, mientras que si concentran sus mayores esfuerzos en la recuperación de su infraestructura.

Se debe resaltar el esfuerzo en empresas de cada segmento en realizar pruebas de penetración a sus perímetros como parte de las auditorías. Esto refleja un cambio en la perspectiva de seguridad por oscuridad que muchas veces se tiene en las redes TO.

Es importante destacar que haya empresas que realicen este tipo de auditorías con lapsos de tres años. Aunque en muchos casos la infraestructura no suele cambiar con el mismo dinamismo que con las redes TI, nuevas vulnerabilidades en dispositivos desplegados surgen día a día y estas deben ser evaluadas con rigor. El hecho que 22 empresas no realicen ninguna auditoría refleja la necesidad de poder incorporar la metodología de un sistema de gestión en la seguridad TO y que se identifique al ejercicio de auditoría como eje fundamental para comprobar que los esfuerzos para el despliegue de soluciones sí son eficaces. (Ver Figura 55).

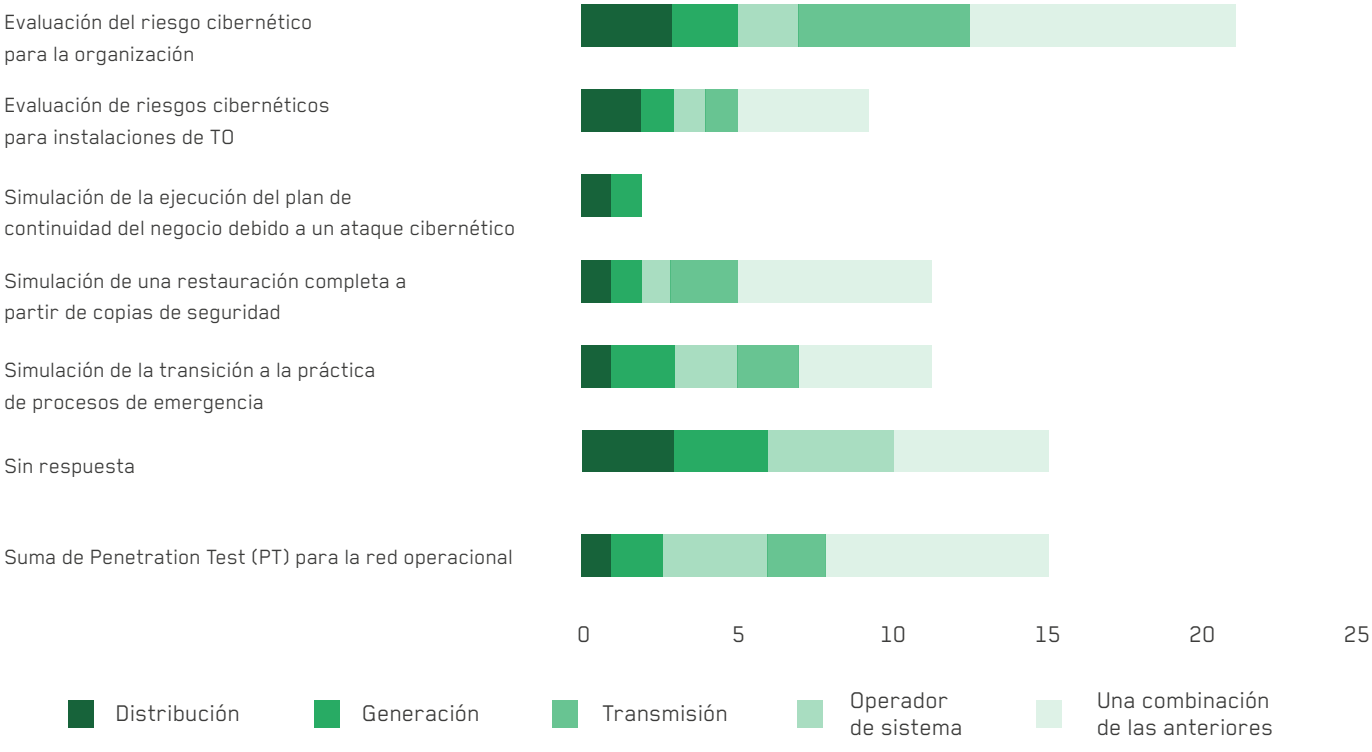


FIGURA 54. Auditoría.

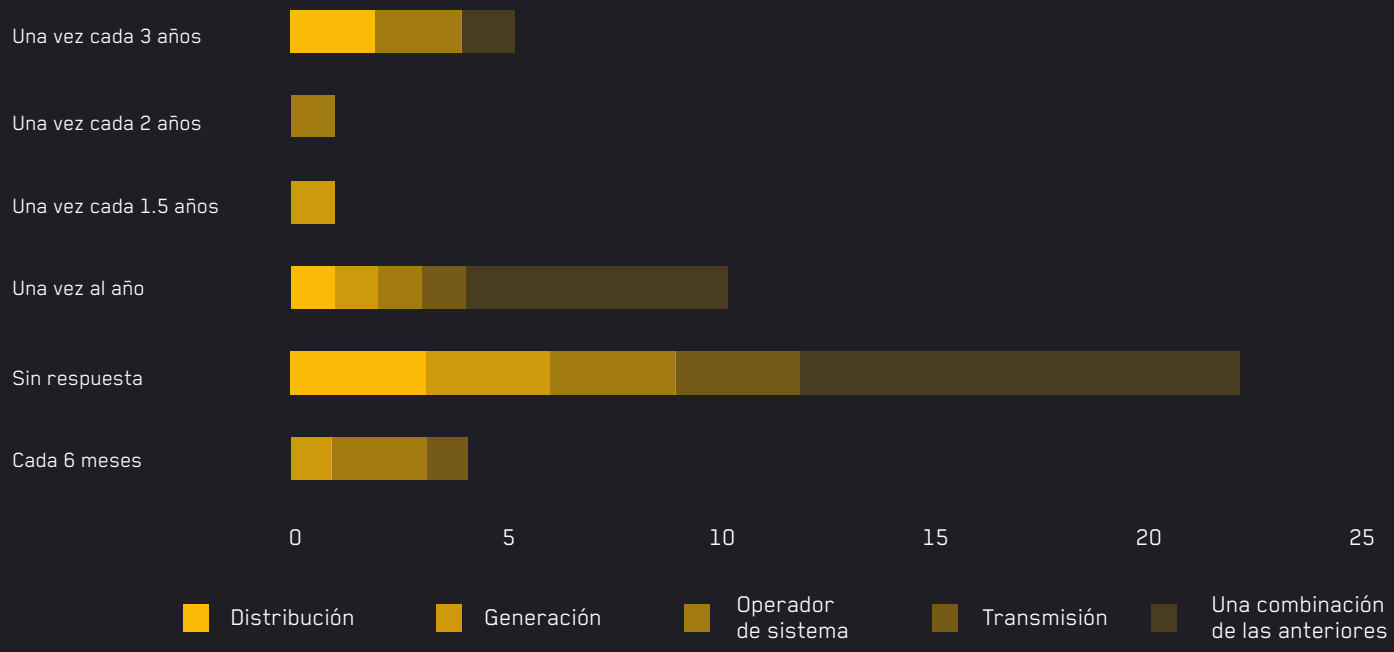


FIGURA 55. Frecuencia auditoría TO.

Tal como se indicó en el inicio de la sección, el compromiso de la alta dirección con la seguridad se refleja en la destinación de recursos, y en este caso del personal idóneo para desempeñar las tareas de salvaguardar la operación de ataques cibernéticos. Se aprecia en la Figura 56 que 13 empresas no han definido este aspecto, mientras que el resto de alguna manera lo tiene especificado. Nuevamente en algunos casos basado en lo definido para TI, y se subraya que sí hay empresas de todos los segmentos consientes de emplear metodologías de TO para definir los roles y responsabilidades.

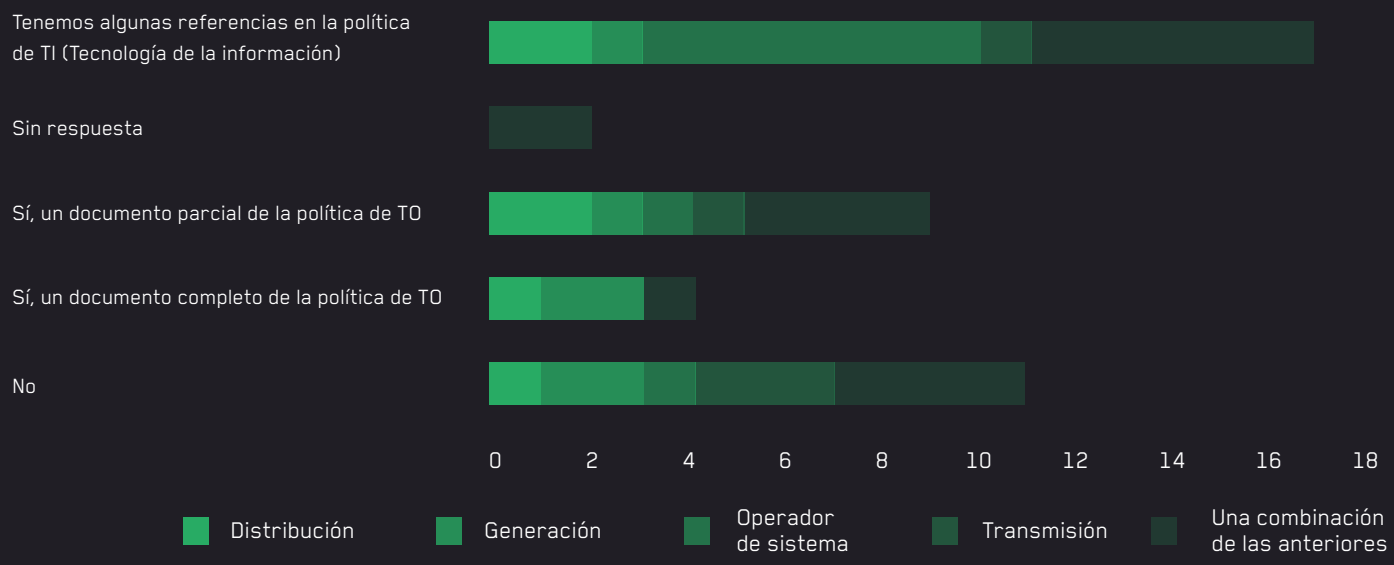


FIGURA 56. Funciones y responsabilidades.

Para el presente estudio se enfatiza en los siguientes roles:

- CISO.
- Encargado regional de seguridad.
- Encargado local de seguridad.
- Equipo de seguridad cibernética.
- Equipo de TO.

Para cada uno de ellos se estudia si está definido y designado y el perfil profesional que han definido para el desempeño del cargo.

Para 18 empresas, este rol no hace parte de su estructura. Para 13 de ellas el cargo desempeña otros roles, mientras que, para el resto, es un cargo de dedicación exclusiva. En relación con su formación, llama la atención que siendo este el mayor cargo en la organización relacionado con la seguridad, 13 empresas consideran que debe ser formado internamente. Esto lleva al dilema de si este es el cargo que debe ser ostentado por el más apto, ¿Cómo dentro de la organización se garantiza que la formación interna es suficiente para desempeñar las funciones deseadas? (Ver Figura 57 y Figura 58)

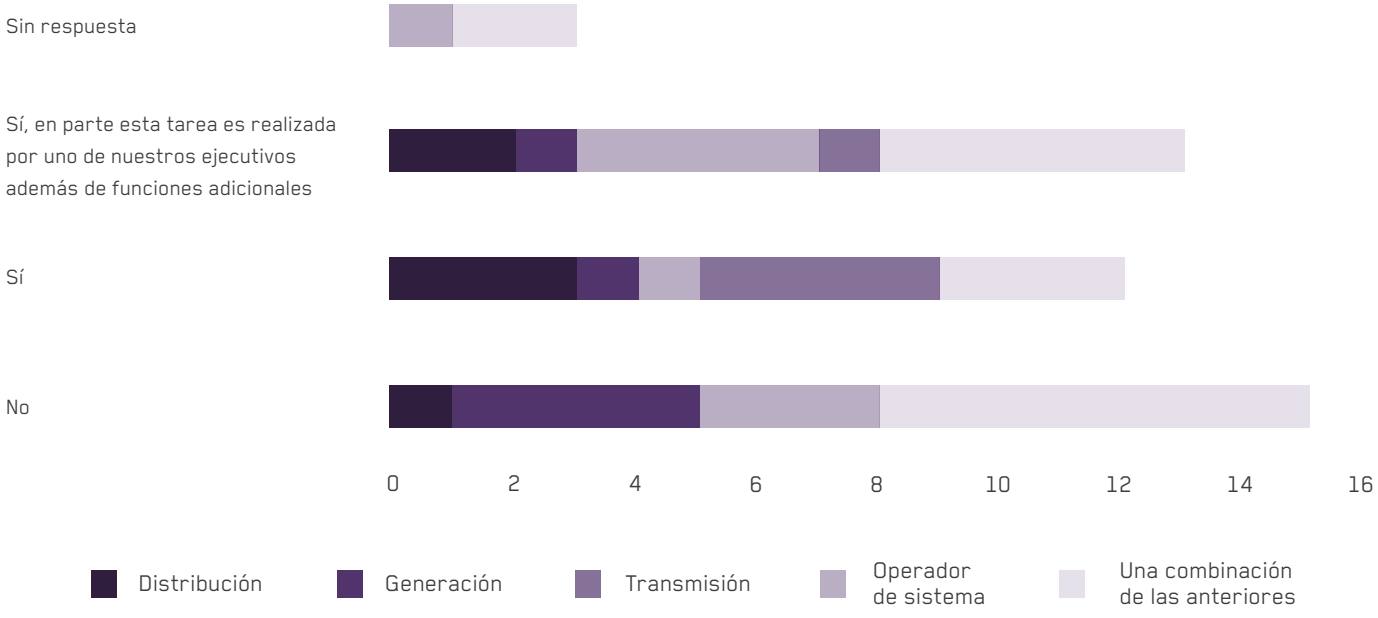


FIGURA 57. Designación del CISO.

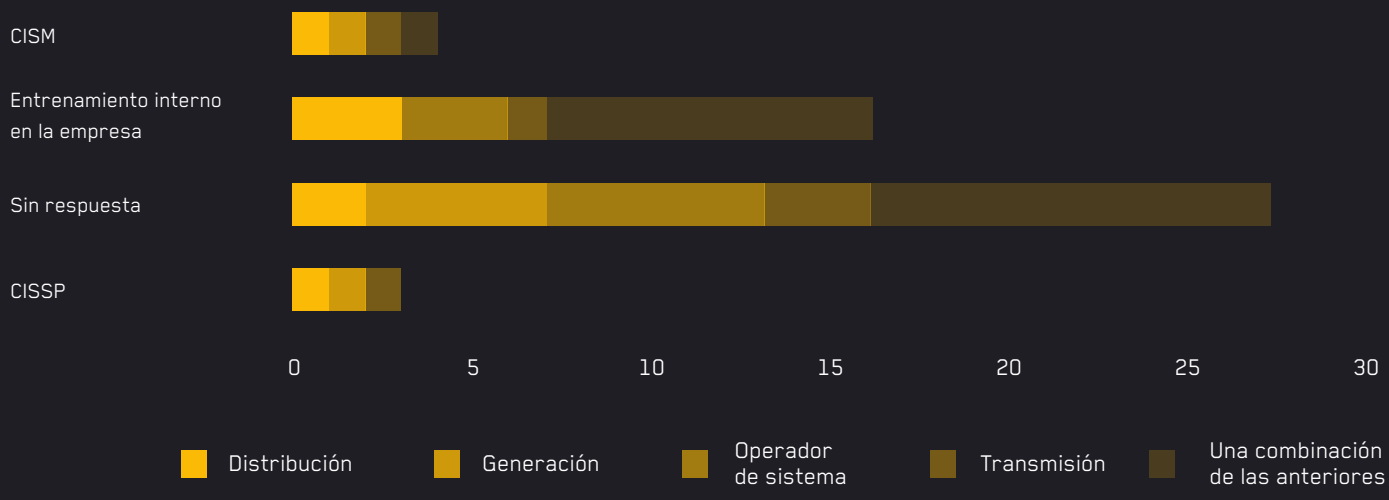


FIGURA 58. Certificación del CISO.

Solamente 6 empresas han definido un encargado regional de seguridad y este cargo es ejercido por personal que ha sido formado internamente en el tema. (Ver Figura 59 y Figura 60)

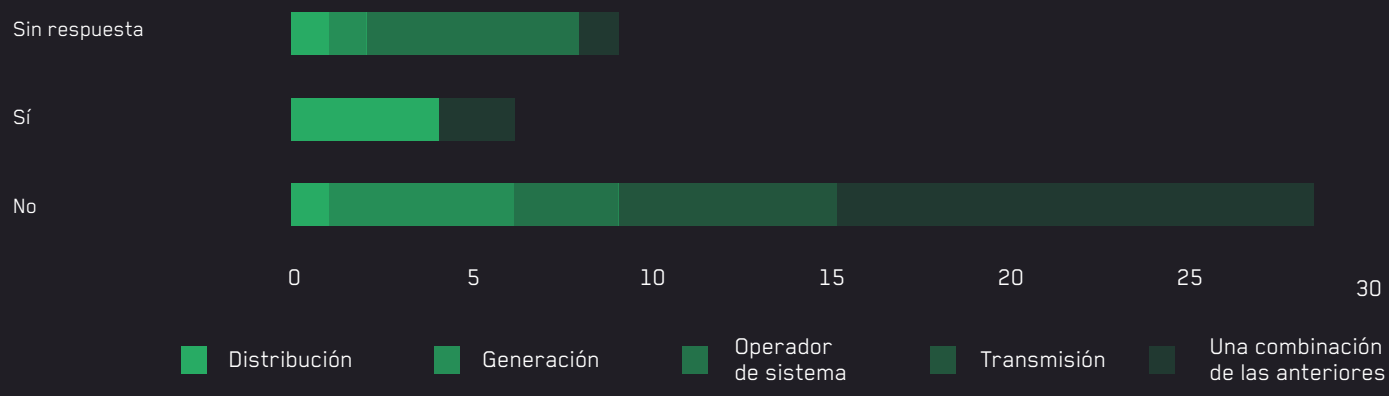


FIGURA 59. Encargado regional de la seguridad en ICS.

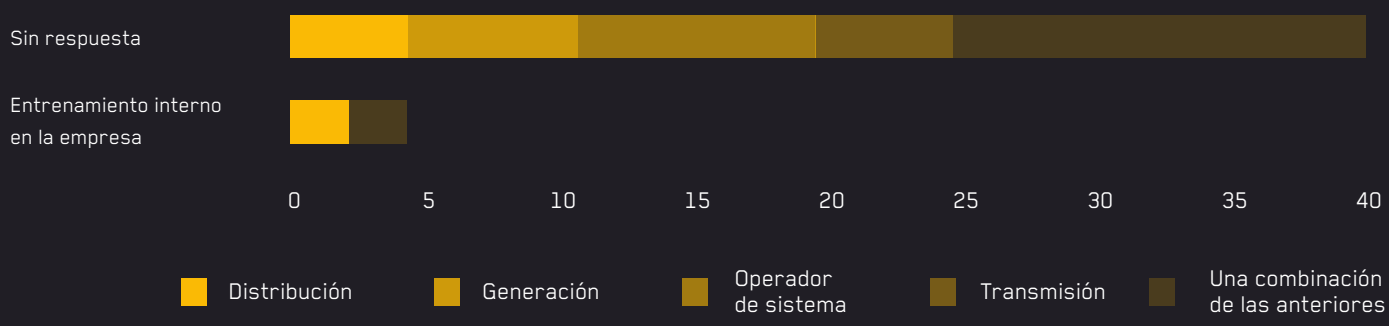


FIGURA 60. Certificación encargado regional de seguridad.

En relación con el encargado local de seguridad en la Figura 61 se indica que tan solo 8 empresas han designado este rol en su organigrama. Nuevamente, para el desarrollo del perfil se requiere de formación al interior de la organización. (Ver Figura 62)

Llama la atención que se dé mucho énfasis a la formación interna por sobre otro tipo de certificaciones en seguridad válidas y específicas de TO. Para garantizar contar con personal actualizado activo y autorizado, esto se logra al incluir la formación de terceras partes reconocidas en el mercado.

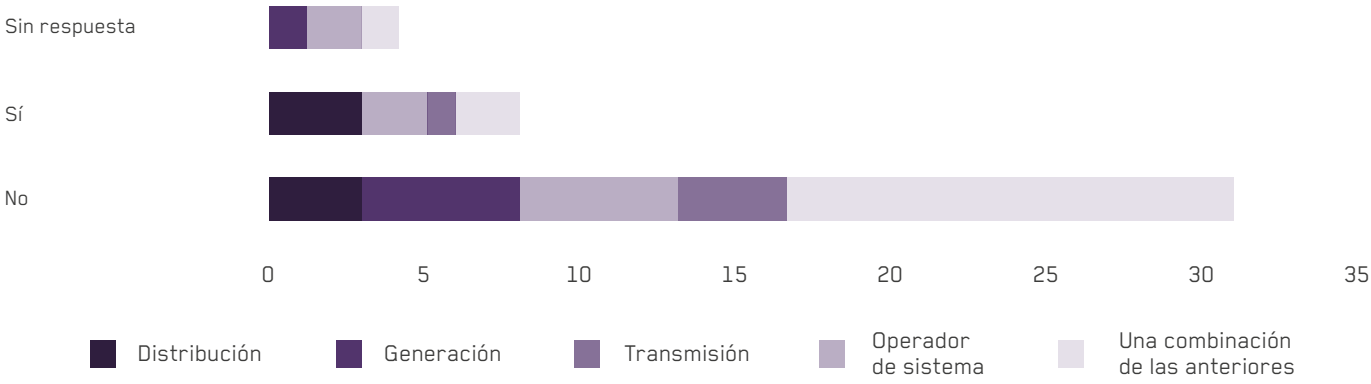


FIGURA 61. Encargado local de seguridad en ICS.

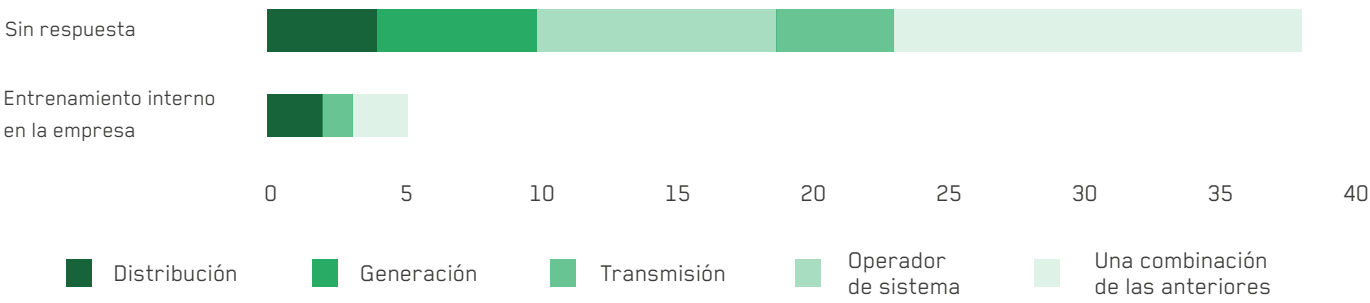


FIGURA 62. Certificación local de seguridad.

Siguiendo esa tendencia a contar con personal formado internamente, está el tener equipos propios que supervisen la seguridad. En gran parte de los casos se aprecia que son equipos de TI que atienden de manera parcial la infraestructura TO. De cierta manera son un CSIRT incipiente que busca darles capacidad a las empresas en la respuesta de incidentes. (Ver Figura 63)

Nuevamente, es extraño ver como la mayoría de las organizaciones indican que no ofrecen formación alguna a su equipo en la respuesta a incidentes. Solo una pequeña porción define capacitación periódica. En relación a la concienciación del personal TO, es notorio que esta no es prioridad en la formación, y quienes lo hacen tienen campañas anuales donde colocan este tema para el equipo de TO. (Ver Figura 64 y Figura 65)

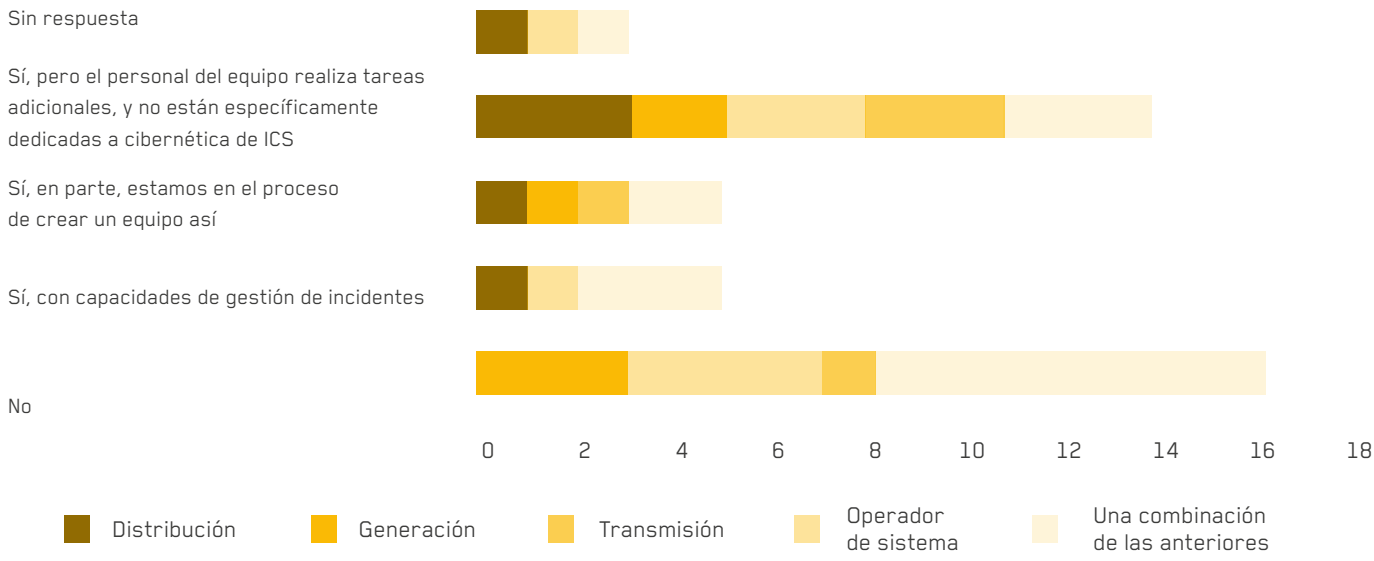


FIGURA 63. Equipo cibernético dedicado para ICS.

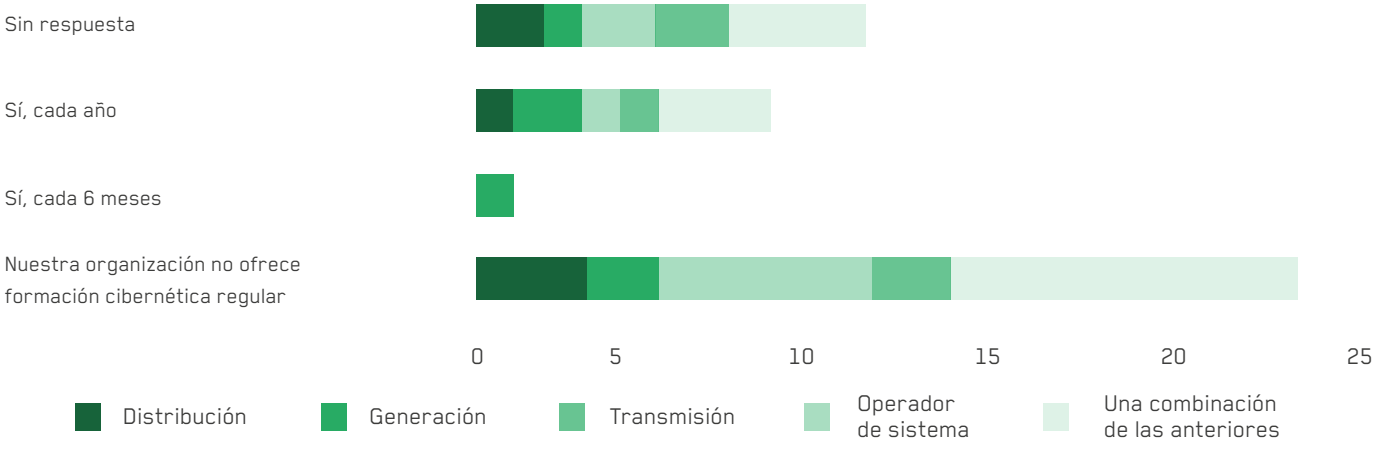


FIGURA 64. Entrenamiento equipo cibernético.

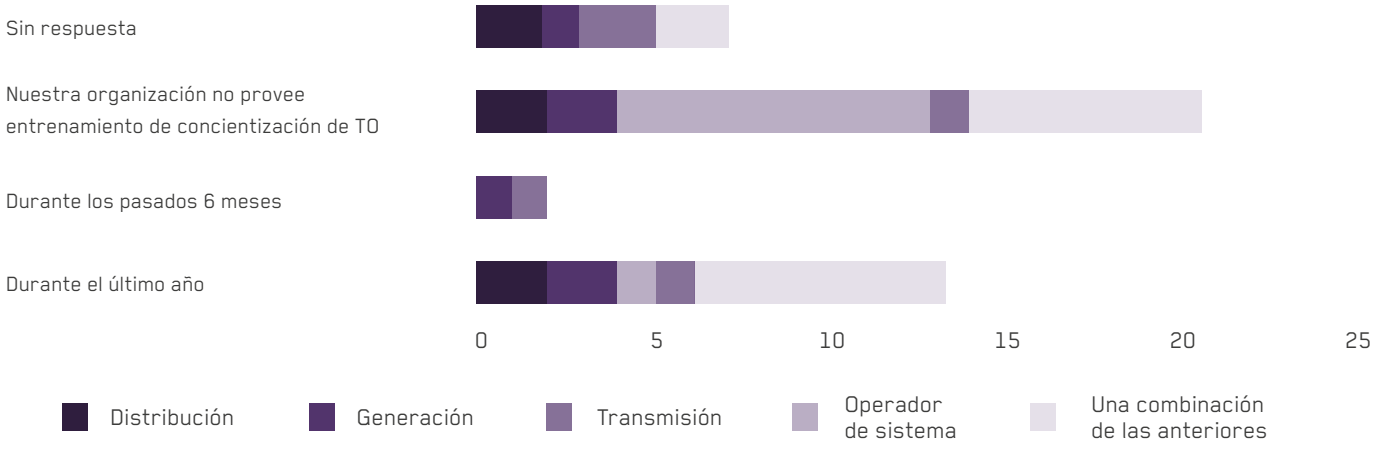


FIGURA 65. Concienciación equipo TO.

3.4.7.2 | *Monitoreo de la seguridad*

Este es uno de los aspectos más llamativos del estudio. Si no se puede medir, no se puede gobernar. No todas las empresas cuentan con una política de monitoreo de su infraestructura TO, pero para quienes sí lo hacen no hay garantía que además de registrar se haga monitoreo del comportamiento de su infraestructura. Puede estarse almacenando los registros de manera continua, pero si no hay analistas procesando dicha información, lo que puede estar ocurriendo nunca será detectado. (Ver Figura 66)

Se aprecia que 11 empresas no monitorean sus redes (Ver Figura 67). Quienes sí lo hacen se reparten entre quienes usan herramientas para ambientes industriales y entre quienes no. Esto quiere decir que la decisión de invertir en herramientas específicas y heredar herramientas de TI es un desafío para resolver. Cuando se profundiza el detalle a la red TO, una porción de los participantes no tiene dicho monitoreo (Ver Figura 68). Para quienes hacen monitoreo, algunos solo lo realizan en horario laboral o simplemente nadie hace seguimiento a las alertas disparadas por las herramientas. Esto evita que pueda hacerse detección temprana de ataques en la red, y que cuando se visibilicen, su impacto sea mucho mayor.

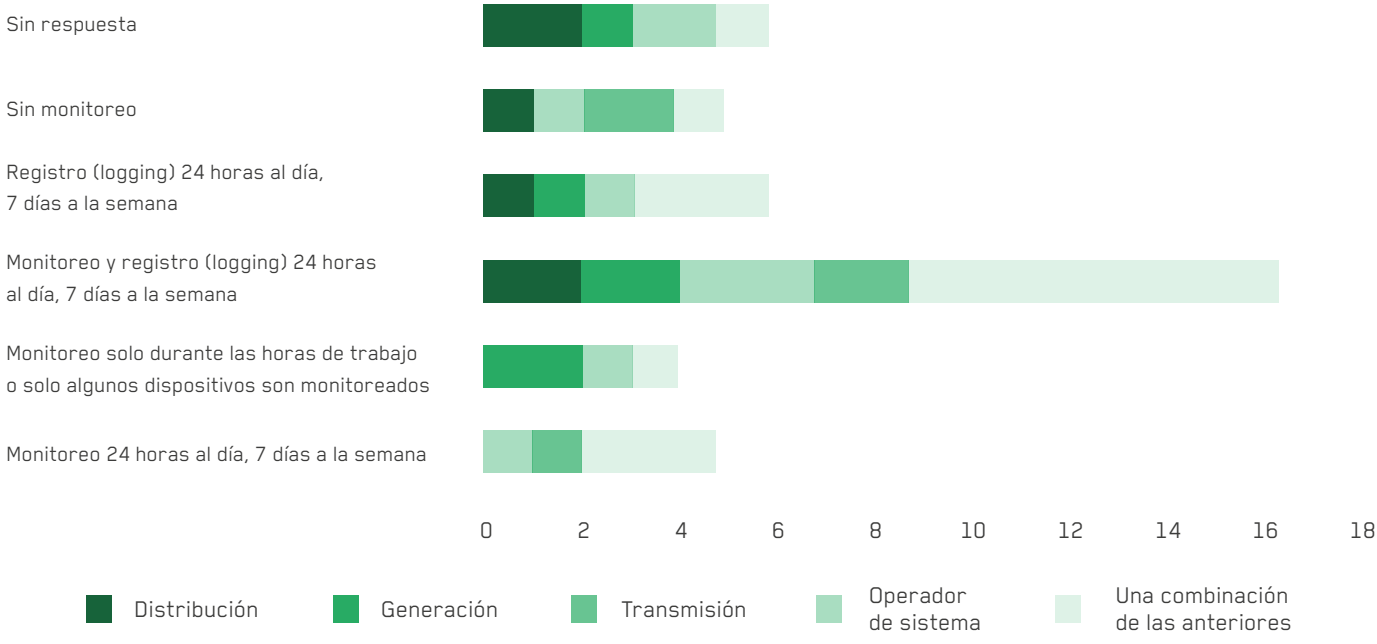


FIGURA 66. Política monitoreo.

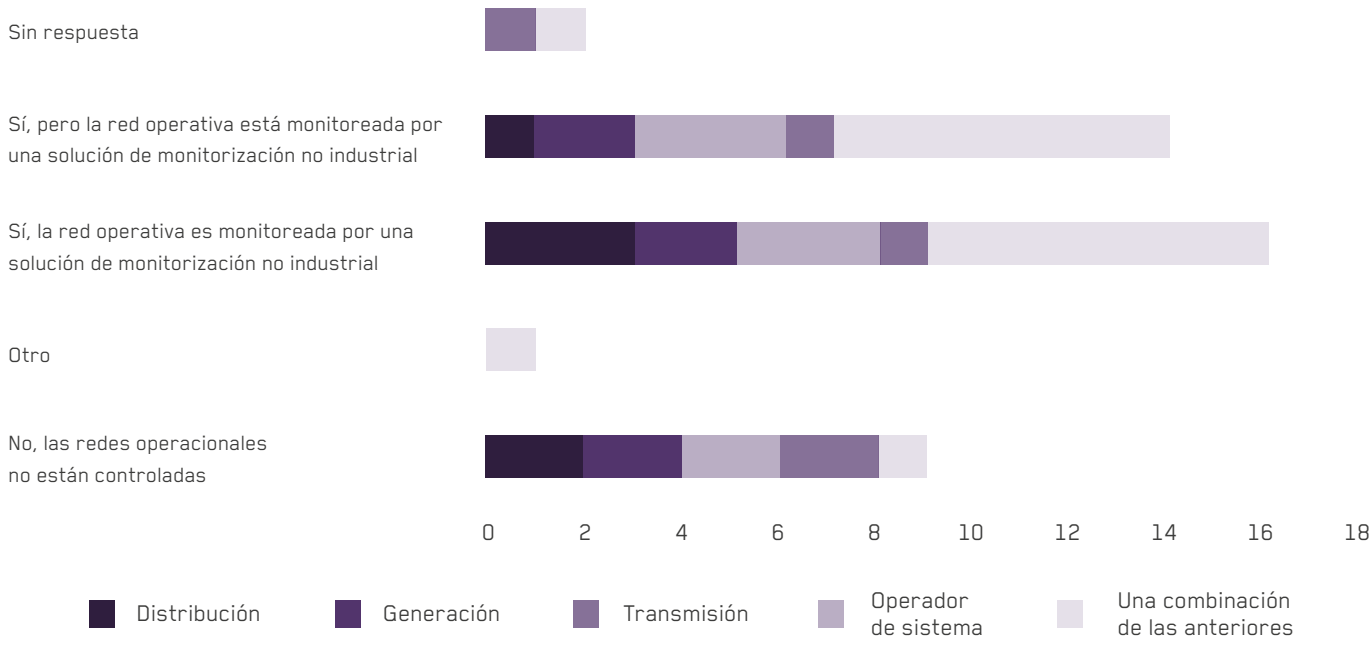


FIGURA 67. Monitoreo red TO.

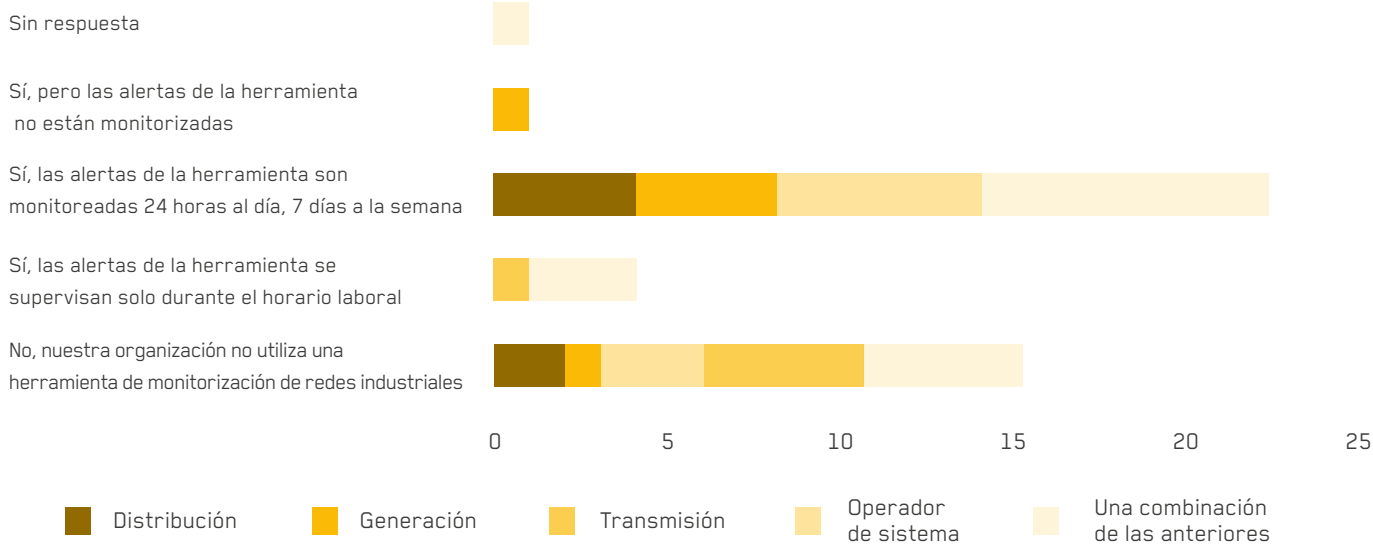


FIGURA 68. Uso de herramientas de monitoreo para redes TO.

¿Qué ocurre cuando una alerta es identificada? (Ver Figura 69) Si hay un equipo dedicado, se dan a la tarea de atenderlo, aun cuando no haya una política definida. Pero aun existiendo la política, sin contar con un equipo, simplemente la alerta no será atendida, y el ataque será respondido cuando su impacto sea mayor. Tan solo 21 empresas cuentan con herramientas para la gestión de incidentes. Esto quiere decir que más del 50% de las empresas no puede hacer una correcta gestión del incidente, es decir, detectar la fuente o causa, definir las acciones para remediarlo y establecer los controles para que no se repita. Esto también afecta su gestión del conocimiento, puesto que no son capaces de definir cómo se comporta su infraestructura y cuál puede ser un comportamiento anómalo. (Ver Figura 70)

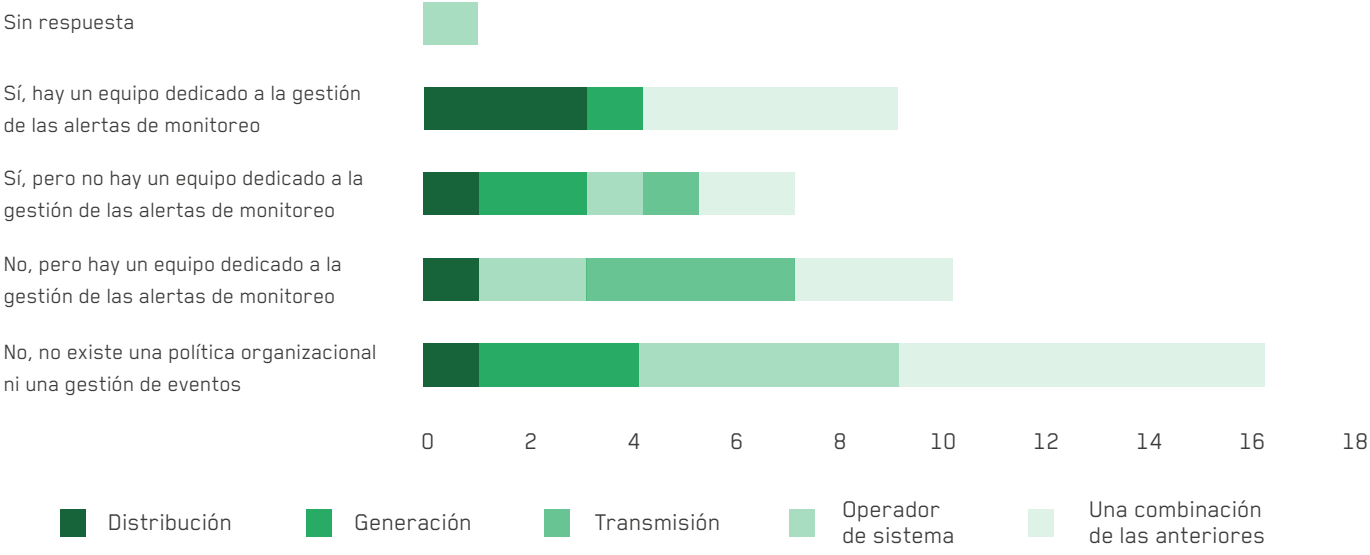


FIGURA 69. Política de gestión de alertas.

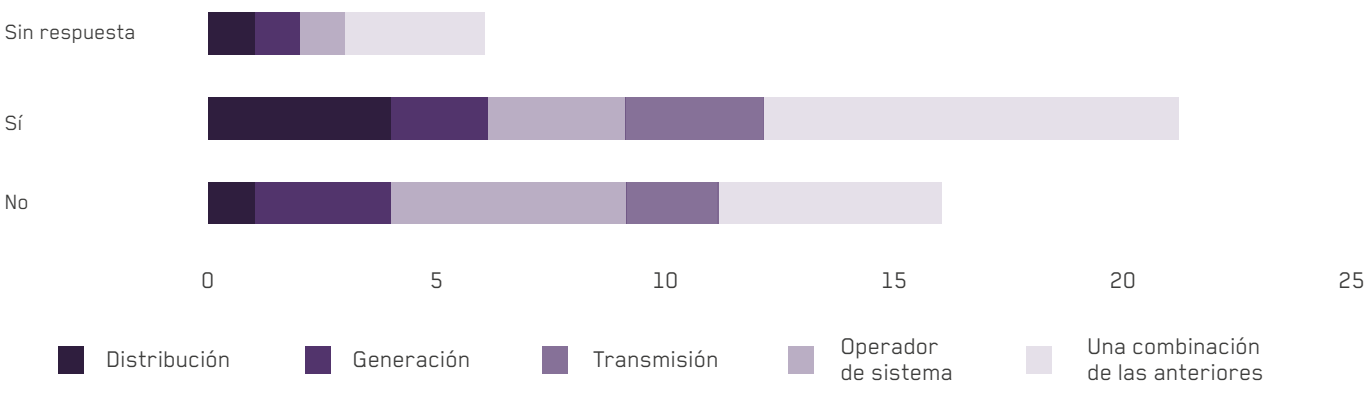


FIGURA 70. Uso de herramientas para la gestión de incidentes.

3.4.7.3 | *Gestión del acceso: físico y lógico*

En cuanto al acceso físico a las instalaciones, en la Figura 71, salvo algunas excepciones, todos tienen medidas que permiten el monitoreo visual de quien está presente. Esto combinado con inspecciones físicas, tienen la posibilidad de ver que ocurre en tiempo real. De manera excepcional, también tienen presencia física con personal las 24 horas, junto con medidas de protección para el acceso a las diferentes áreas. (Ver Figura 72)

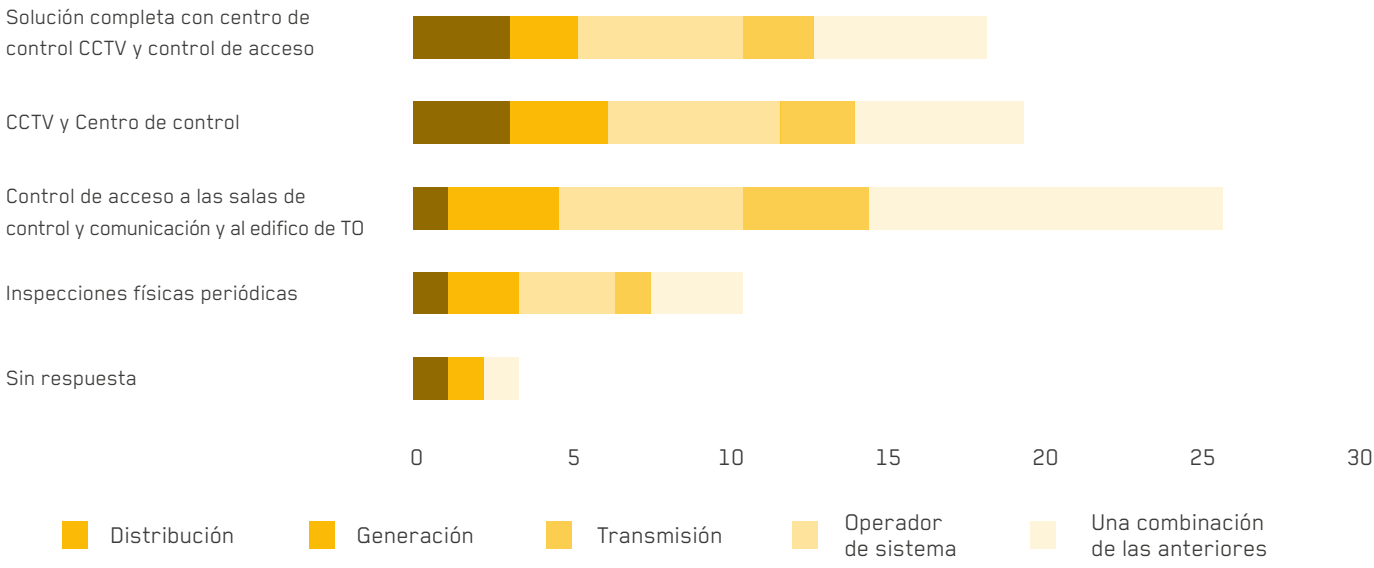


FIGURA 71. Control acceso físico TO.

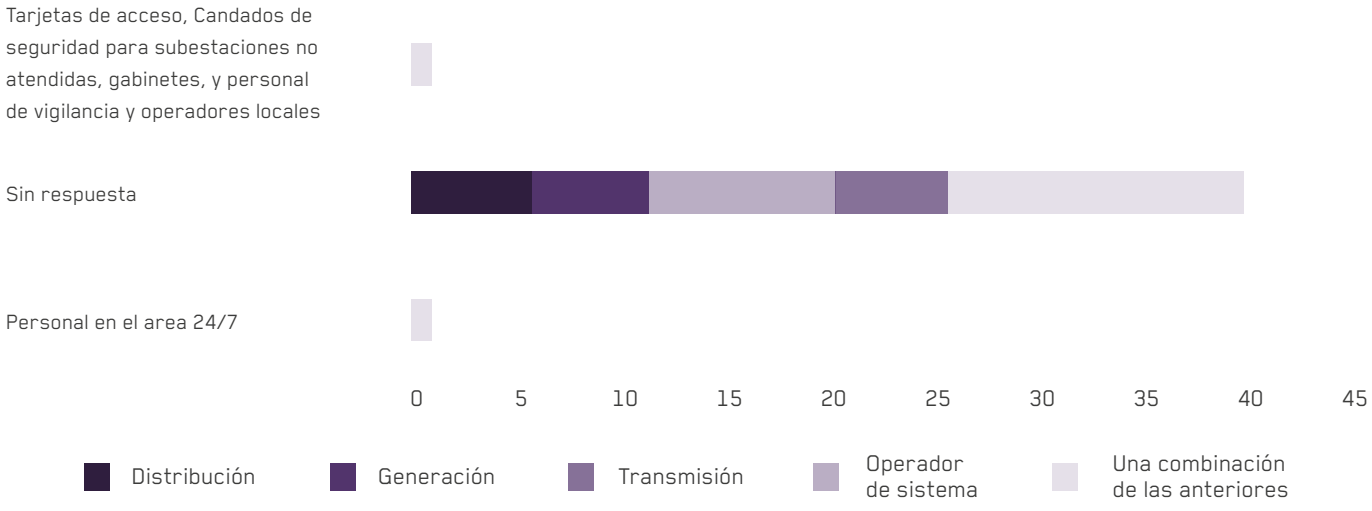


FIGURA 72. Otros mecanismos de acceso físico.

En cuanto a la autorización de visitantes externos, hay procesos informales y otros documentados relacionado con quien puede autorizar el ingreso. Siempre es requerido un permiso de acceso a las instalaciones. (Ver Figura 73)

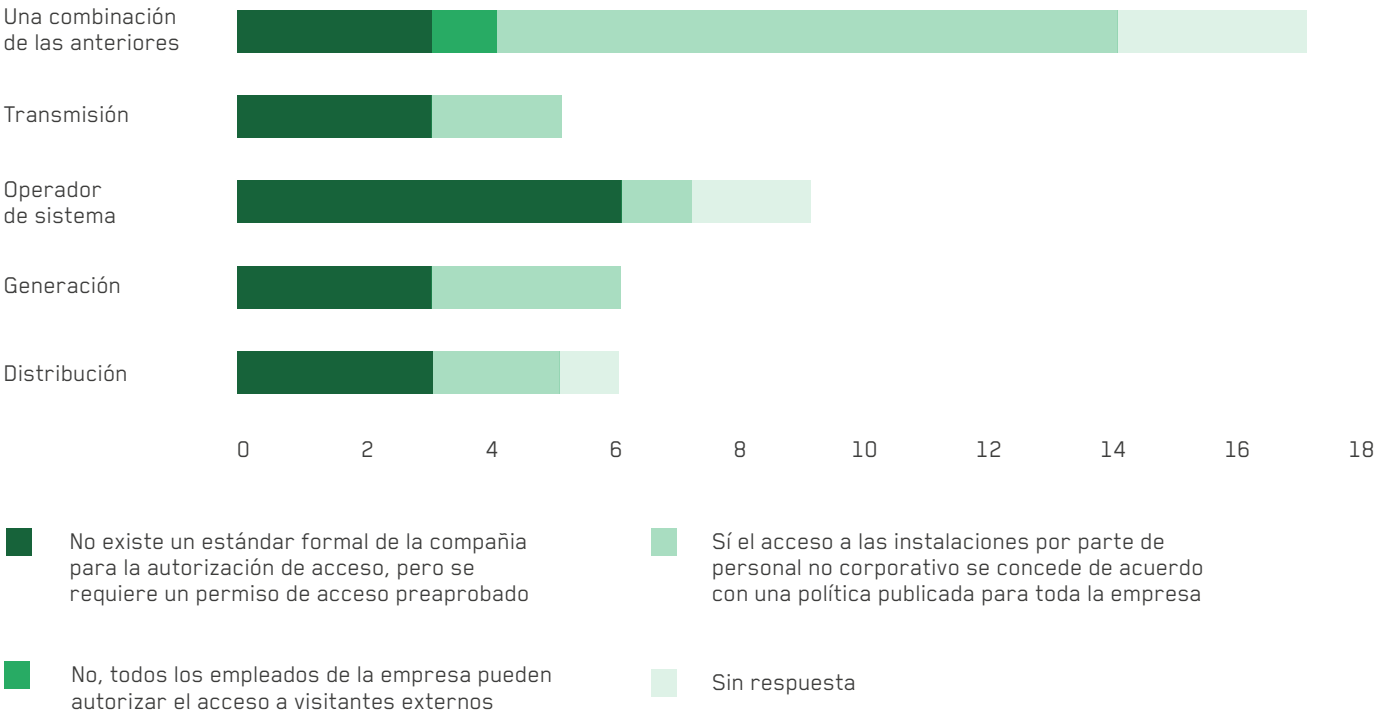


FIGURA 73. Control de acceso para visitantes externos.

Aunque todo visitante requiere que se tenga un permiso gestionado, llama la atención el caso de invitados por parte de ejecutivos (C-Level) que no siempre tienen acompañante de seguridad (Figura 74). Esto abre la oportunidad a ataques explotando dicha vulnerabilidad.

Desde la parte física se guardan los registros de quienes visitan. Esto hace parte de los protocolos de seguridad física, los cuales, en muchos casos a ser provistos por terceras partes, hacen parte de su forma de operar. (Ver Figura 75)

En la Figura 76 se enuncia que los activos en las instalaciones son protegidos de un acceso físico no autorizado. Esto puede ser por parte de personal interno o externo, y hace parte de la estrategia de seguridad por capas.

Todo esto contrasta con el acceso lógico a las instalaciones de TO (Ver Figura 77). El acceso puede ser por medio de equipo propios de la empresa o de sus contratistas, pero siempre bajo su custodia. Pero hay una práctica muy marcada donde el contratista trae su equipo y lo conecta a la red sin ningún límite. Estos equipos pueden comprometer la red y este riesgo parece no haber sido evaluado.

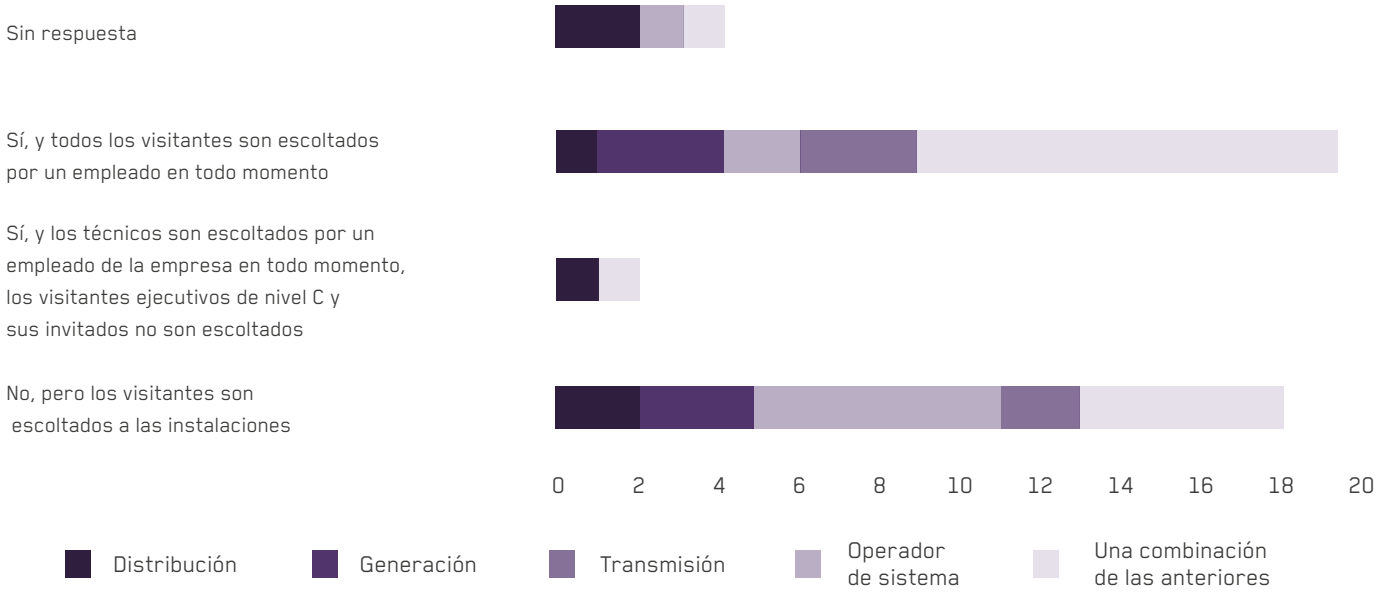


FIGURA 74. Procedimiento para los visitantes.

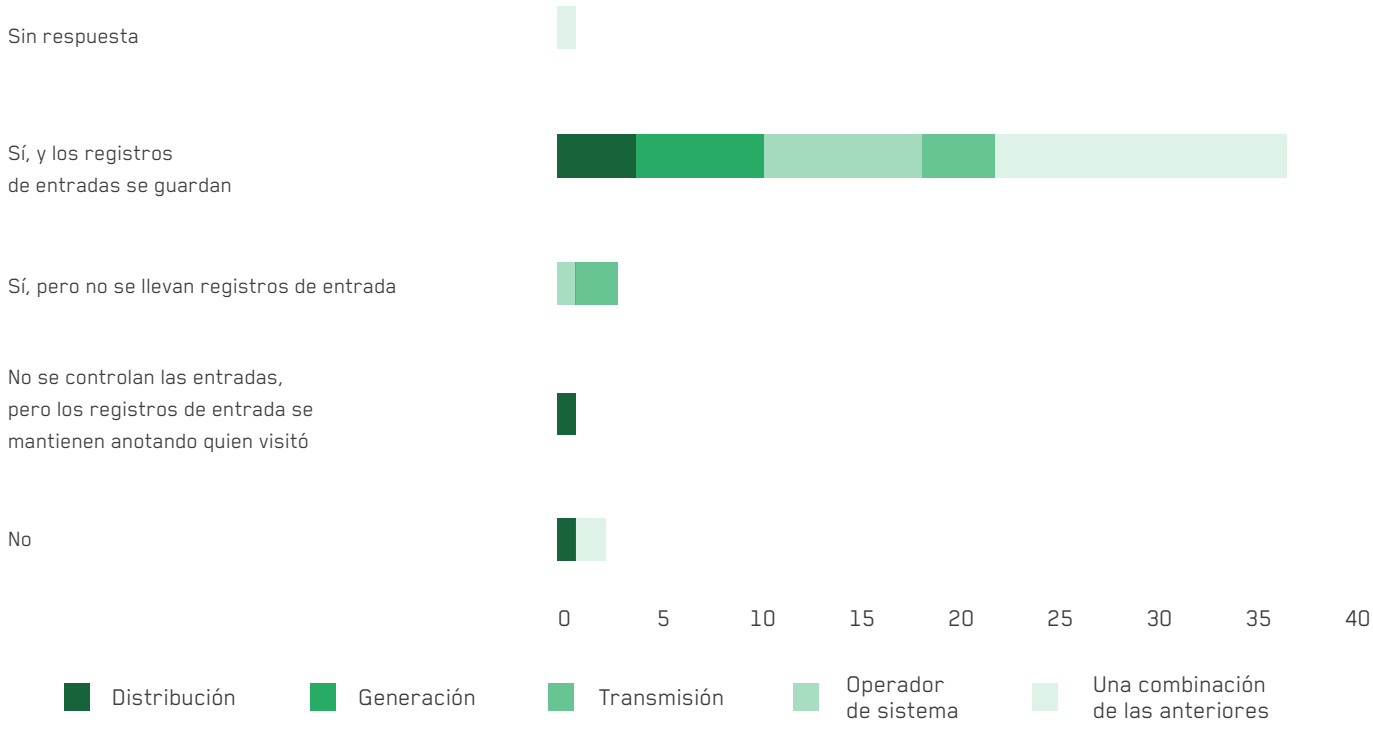


FIGURA 75. Control de llegada y salida de visitantes.

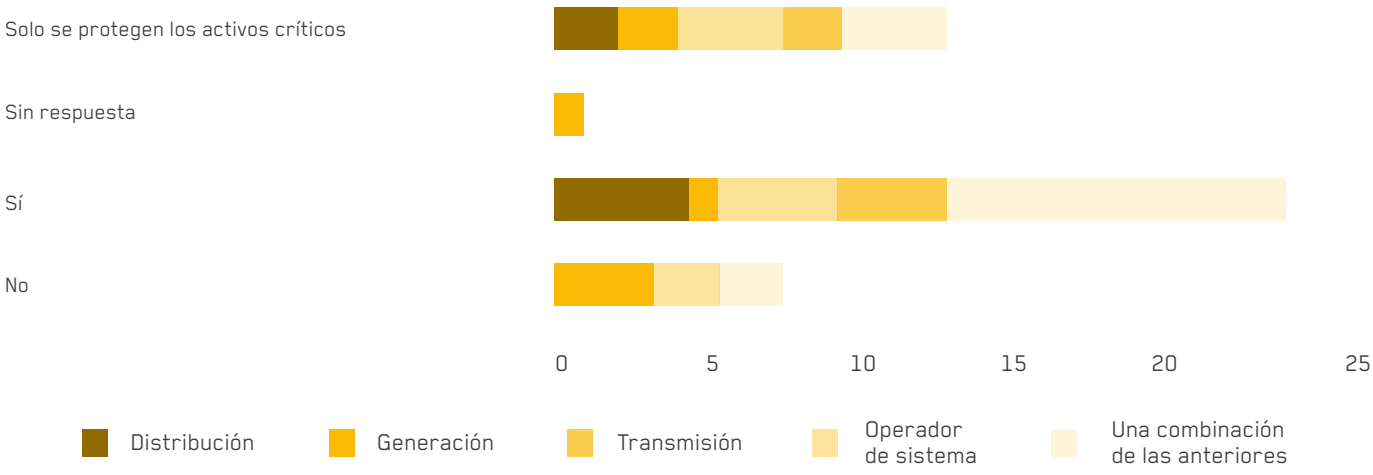


FIGURA 76. Bloqueo de acceso físico a los activos de TO.

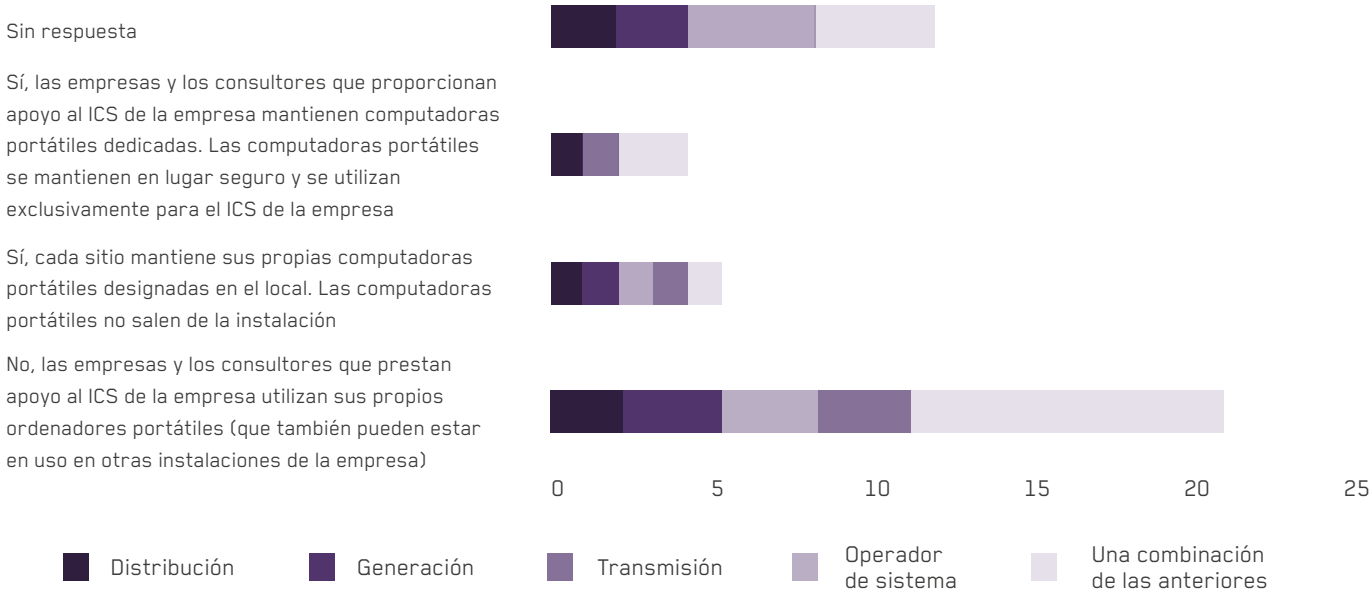
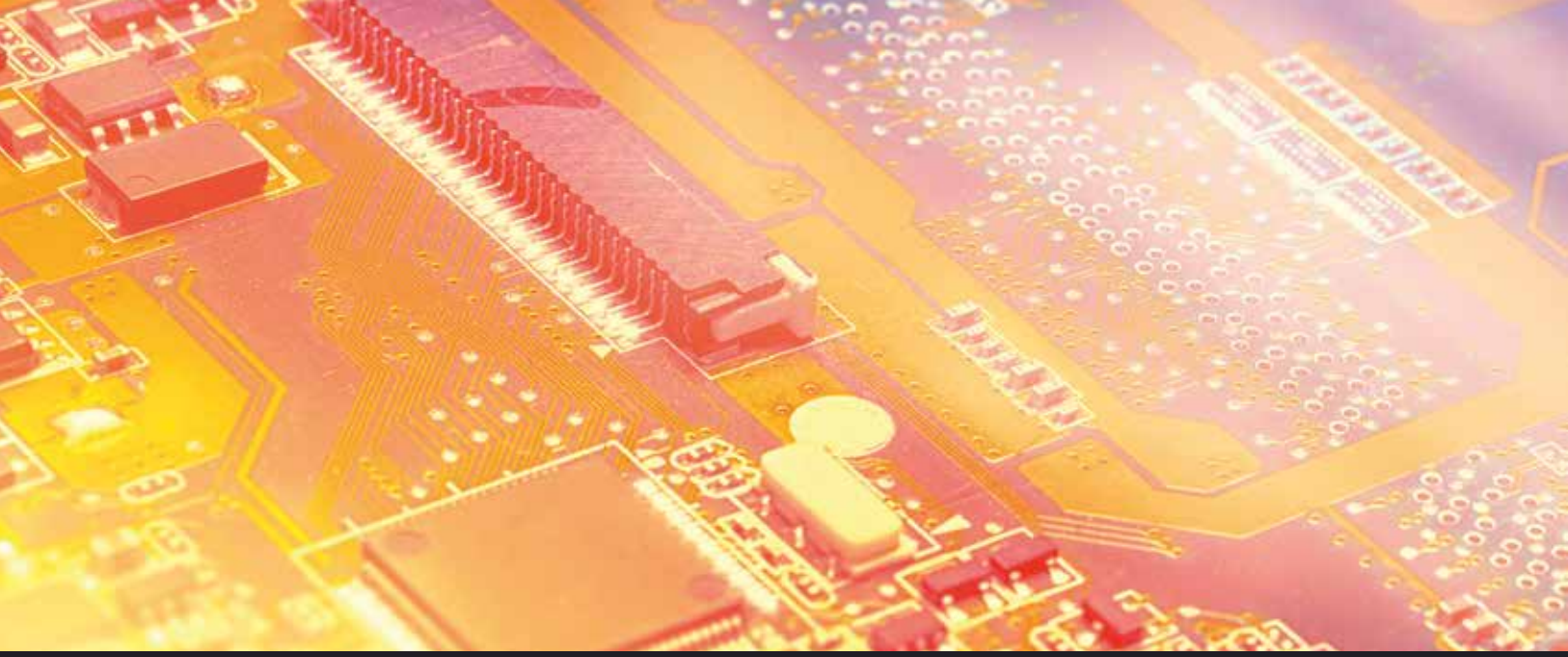


FIGURA 77. Uso de equipos de terceros en la red TO.

Llama la atención como hoy **está permitido** para este tipo de **infraestructura crítica** el acceso remoto **a sus redes**

Se apoyan para la autenticación de los usuarios en la plataforma de TI (ver Figura 78), de tal manera que por medio de un directorio activo se autentican la mayoría de los usuarios.

Toda creación de nuevos usuarios es supervisada, ya sea de manera manual o automatizada. (Ver Figura 79)



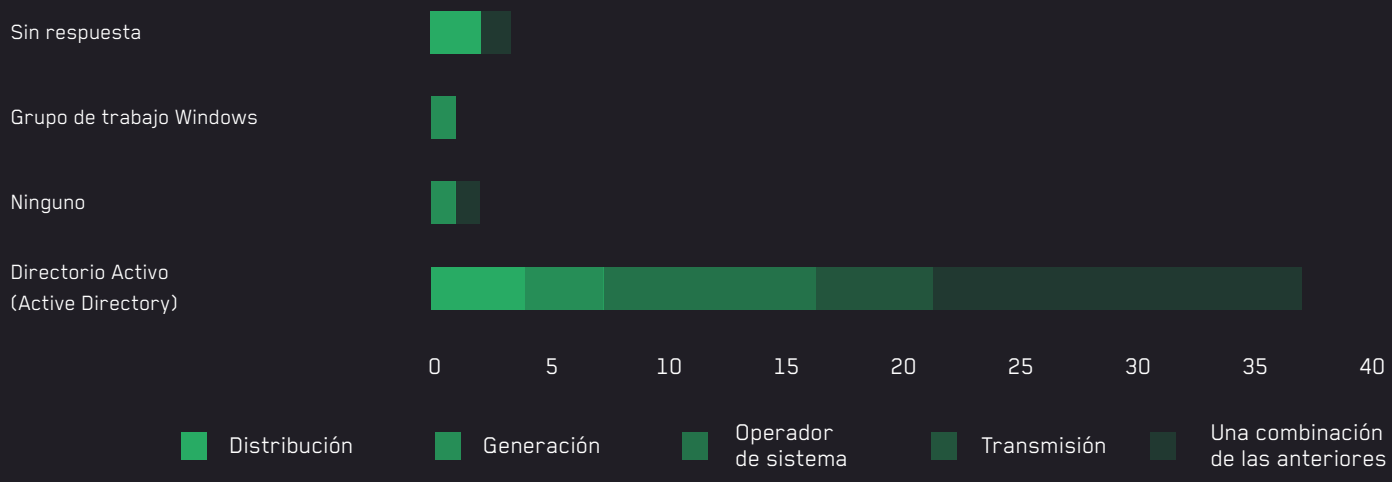


FIGURA 78. Autenticación de usuarios.

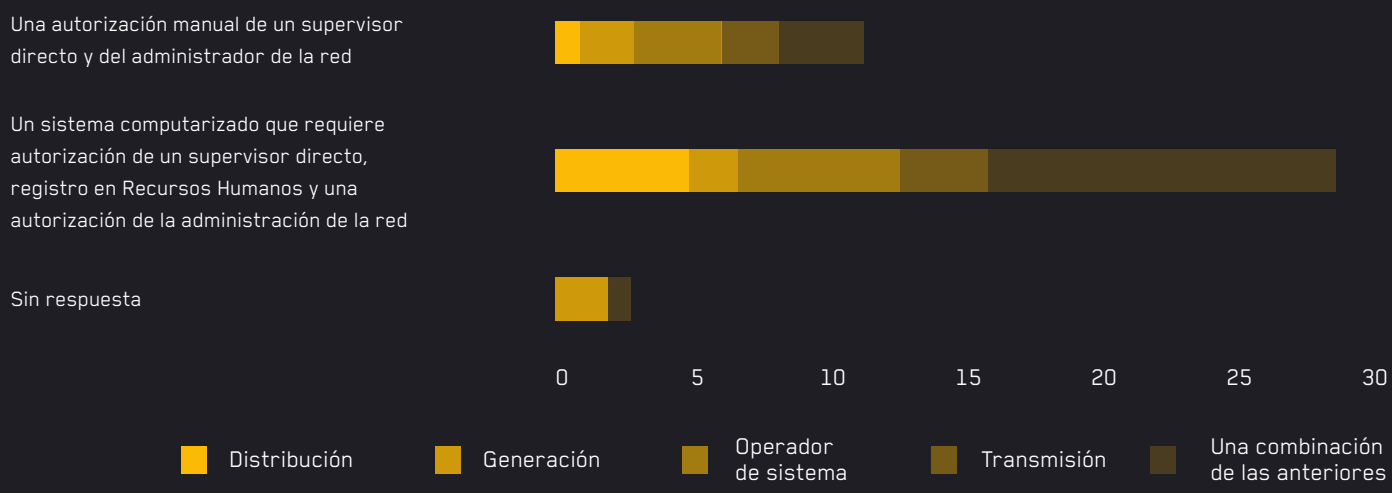


FIGURA 79. Política de creación de nuevos usuarios.

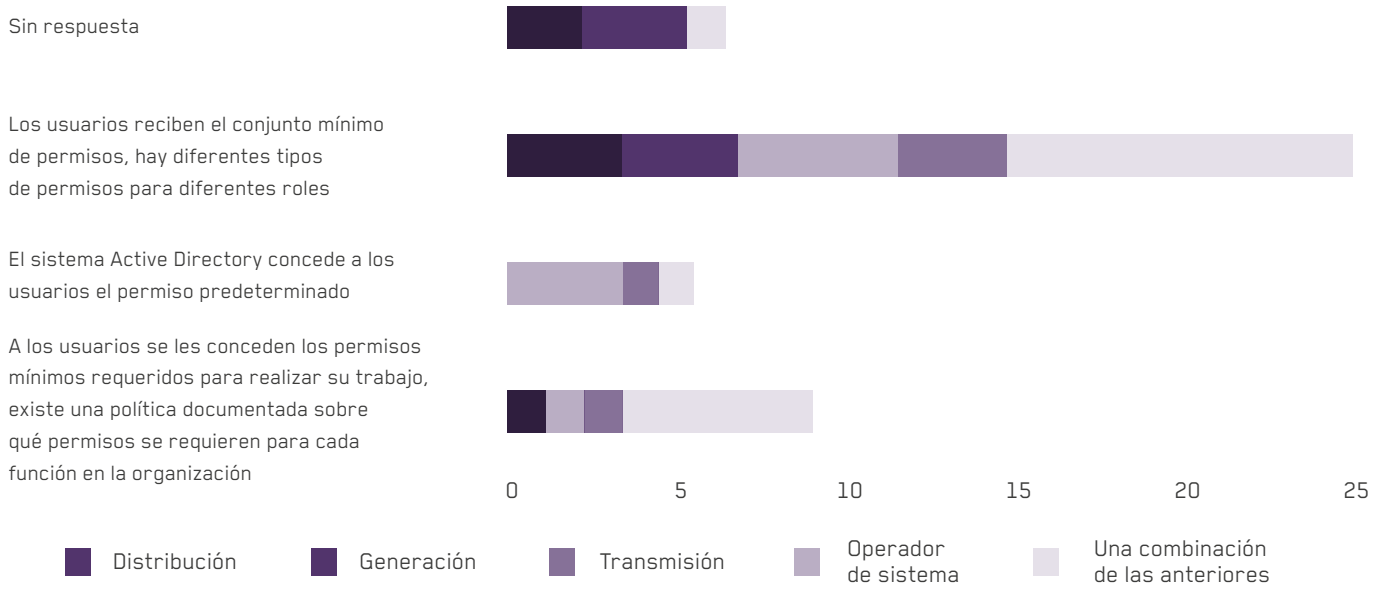


FIGURA 80. Gestión de permisos de acceso.

La Figura 80 denota la ausencia de sistemas AAA (Autenticación, autorización y auditoría), puesto que está muy fragmentado el proceso de gestión de permisos coherente con las necesidades y la supervisión para la generación y asignación de perfiles.

Llama la atención como hoy está permitido para este tipo de infraestructura crítica el acceso remoto a sus redes (Ver Figura 81). Esto va desde la posibilidad de que cualquier usuario lo pueda hacer, hasta contar con procesos informales o documentados que indiquen quienes sí tienen dicho privilegio. Para proteger esta conexión remota, se emplean múltiples técnicas (ver Figura 82), siendo la más común el uso de firewall de extremo a extremo. Esto indica el cifrado del canal, pero no garantiza el cifrado del mensaje. Se evidencia la ausencia de múltiples factores de autenticación para equipos de función crítica.

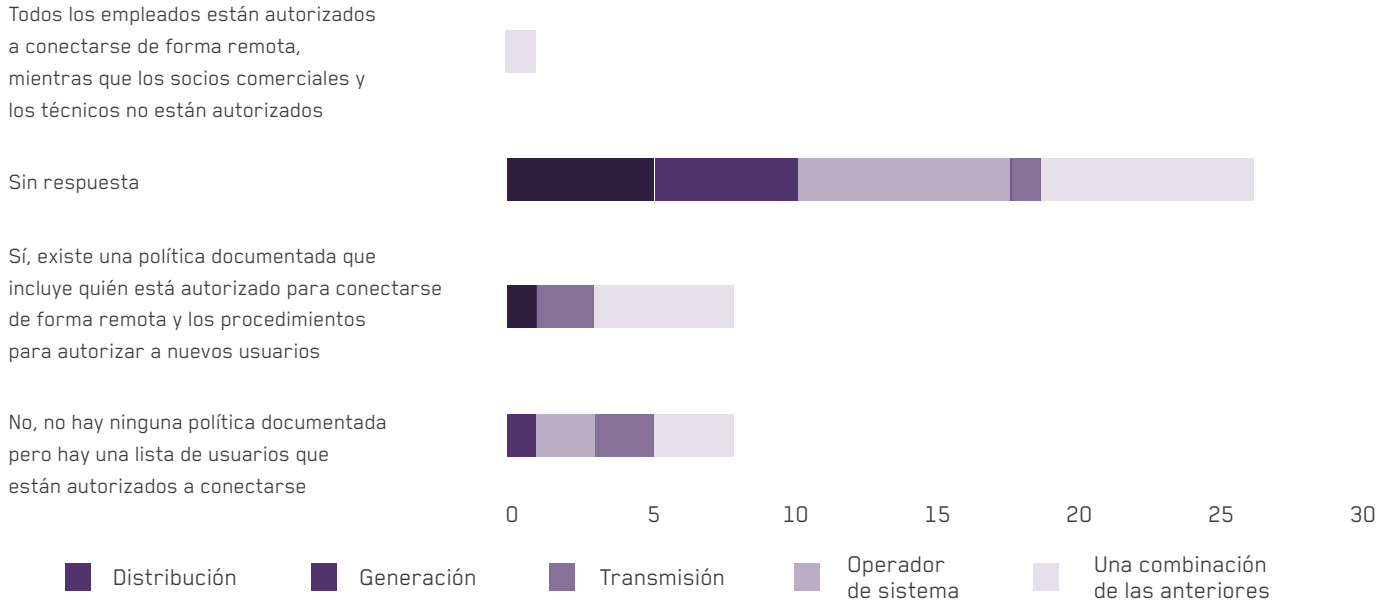


FIGURA 81. Política de conexión remota.

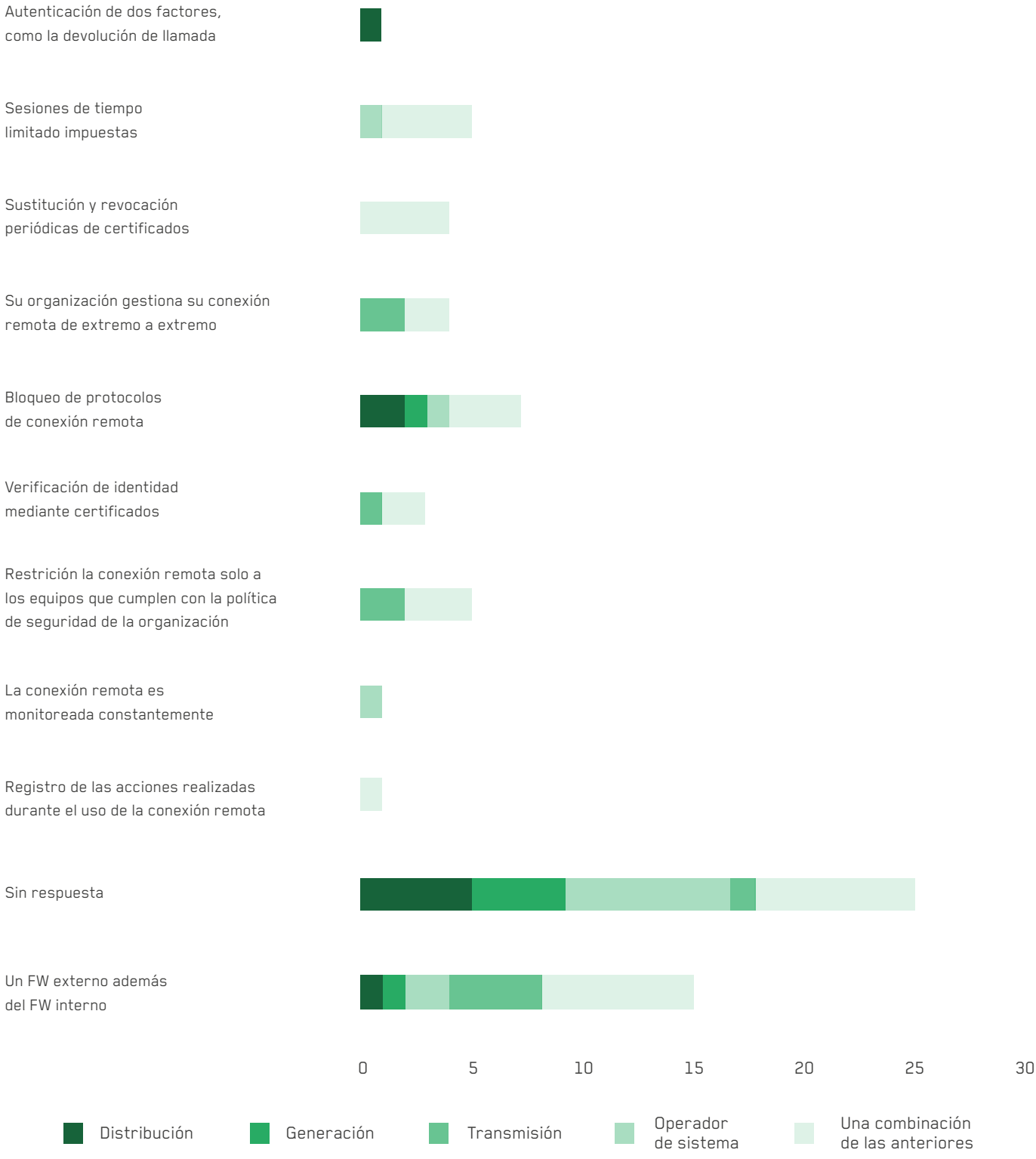


FIGURA 82. Controles conexión remota.

3.4.7.4 | *Actualización y bastionado*

En este punto se compara la existencia de una política de bastionado, con la actualización del firmware como uno de los procedimientos a ser implementados. Para ello se evalúa los siguientes equipos:

- PLC (Figura 83 y Figura 84)
- Estaciones de ingeniería (Figura 85 y Figura 86)
- Servidores de control (Figura 87 y Figura 88)
- Equipos de red (Figura 89)
- EPS (Figura 90)

Es evidente, en general, la relación entre quienes no disponen de políticas y quienes no actualizan nunca el firmware. Esto refleja que no hay un ejercicio de gestión del riesgo donde se resalte la necesidad de aplicar parches de actualización a los diversos firmware disponibles (actualizaciones de desempeño o de seguridad).

Para el caso de los PLC, esta actividad no hace parte de su cotidianidad, y pocas empresas emprenden dicha tarea. Casos similares se encuentran con las estaciones de ingeniería y los servidores de control. Esto refleja la estrategia de seguridad por oscuridad, ya que, si no está supuestamente expuesto, no se requiere hacer nada por el equipo. Esto expone a todos los componentes a ser atacados explotando vulnerabilidades antiguas para las cuales existen parches, pero que nunca se han colocado.

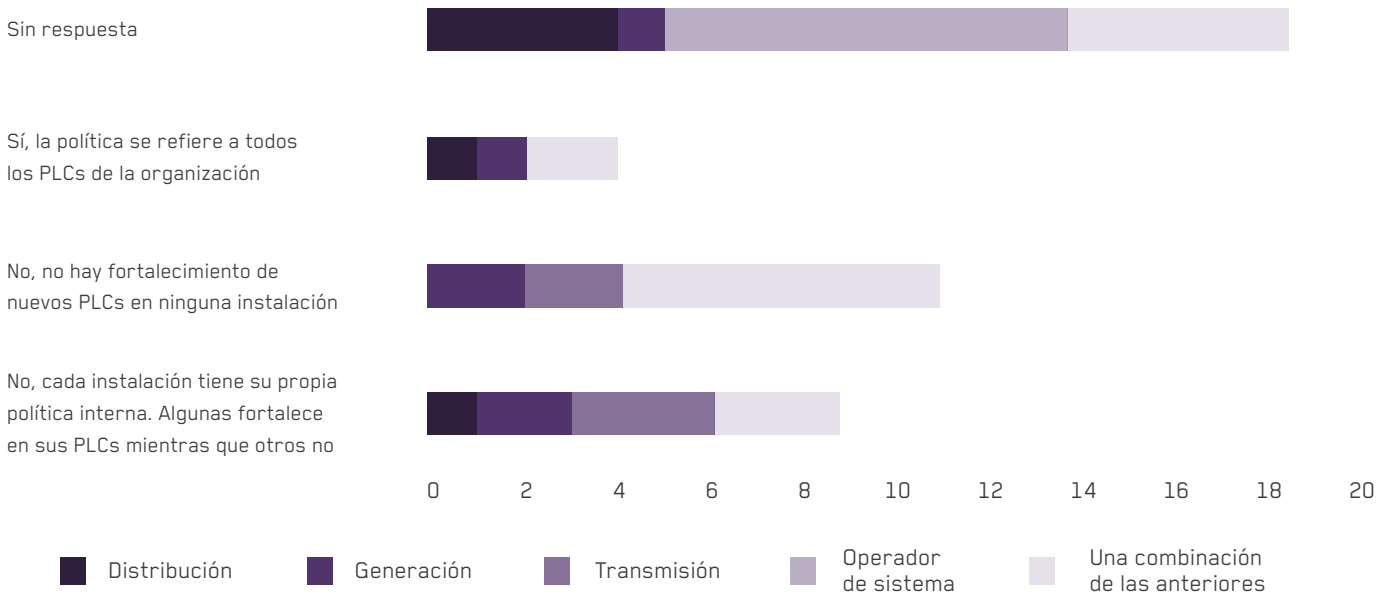


FIGURA 83. Política bastionado PLC.

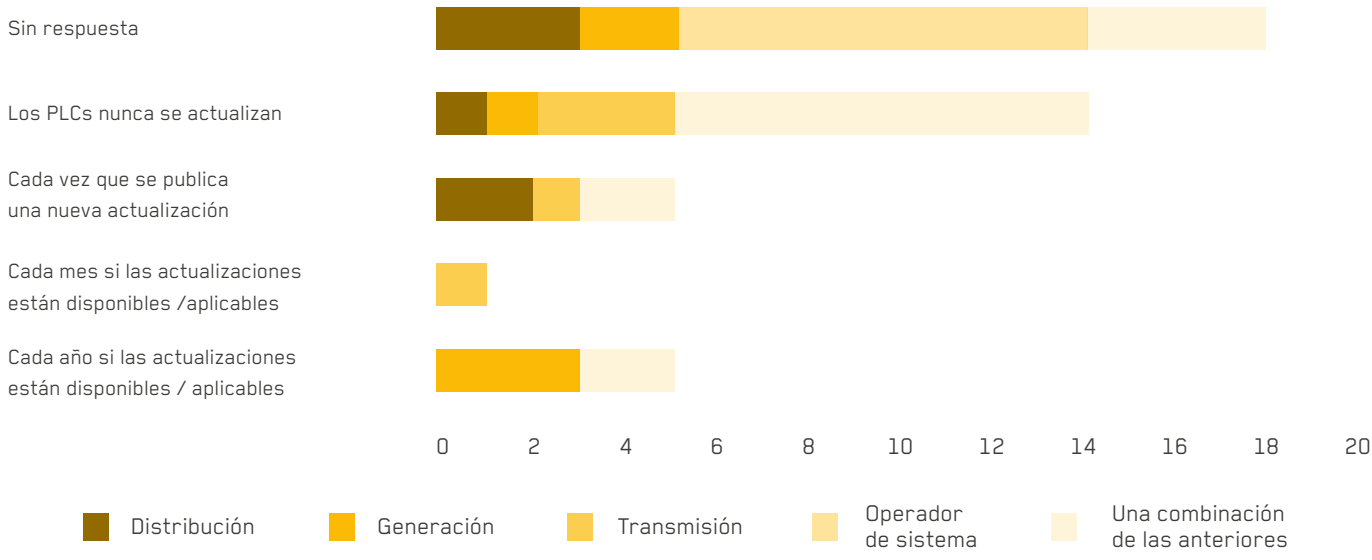


FIGURA 84. Actualización firmware PLC.

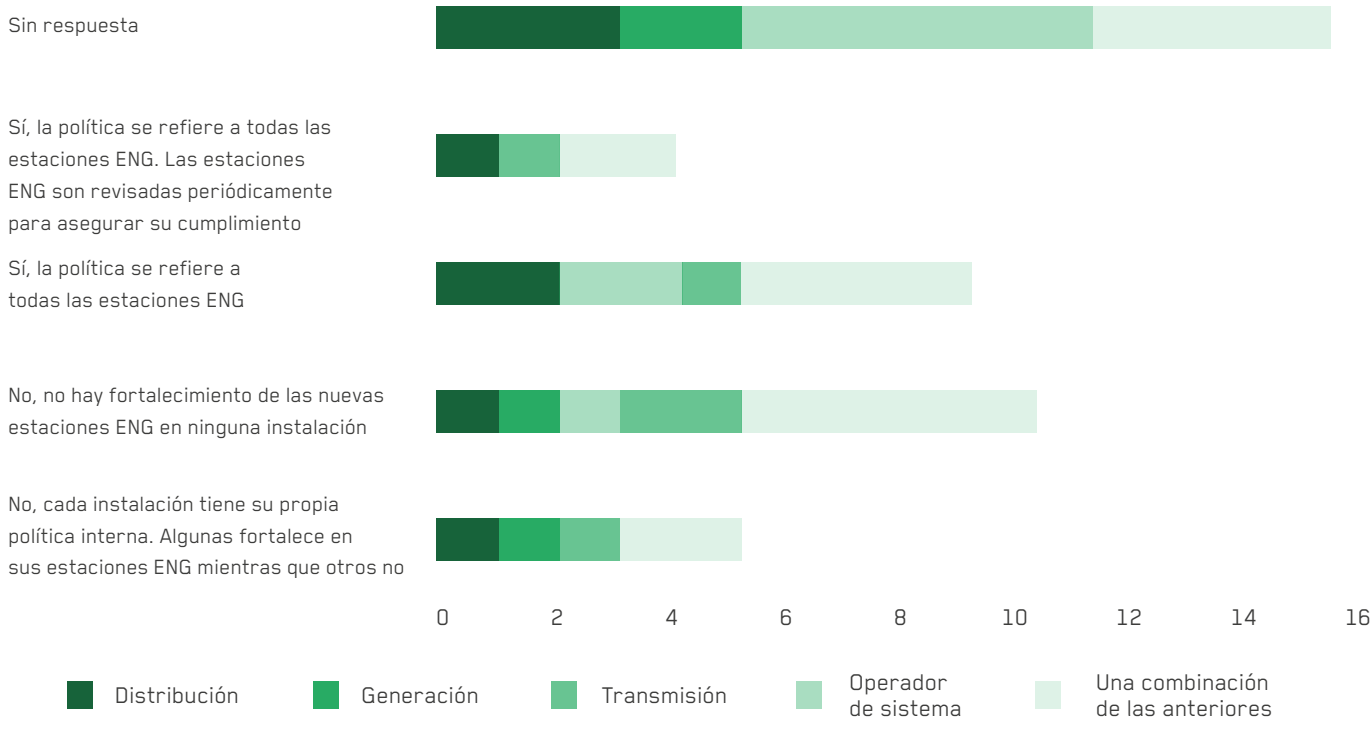


FIGURA 85. Política Bastionado estaciones de ingeniería.

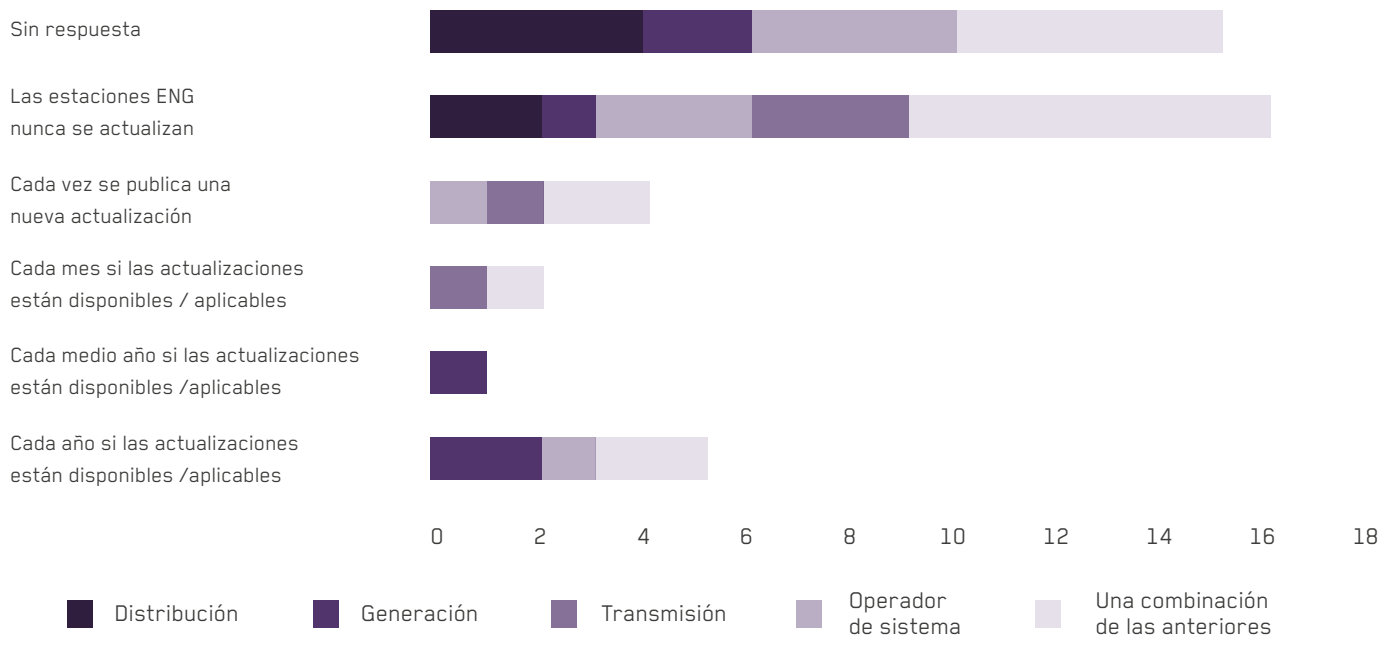


FIGURA 86. Actualización firmware estaciones de ingeniería.

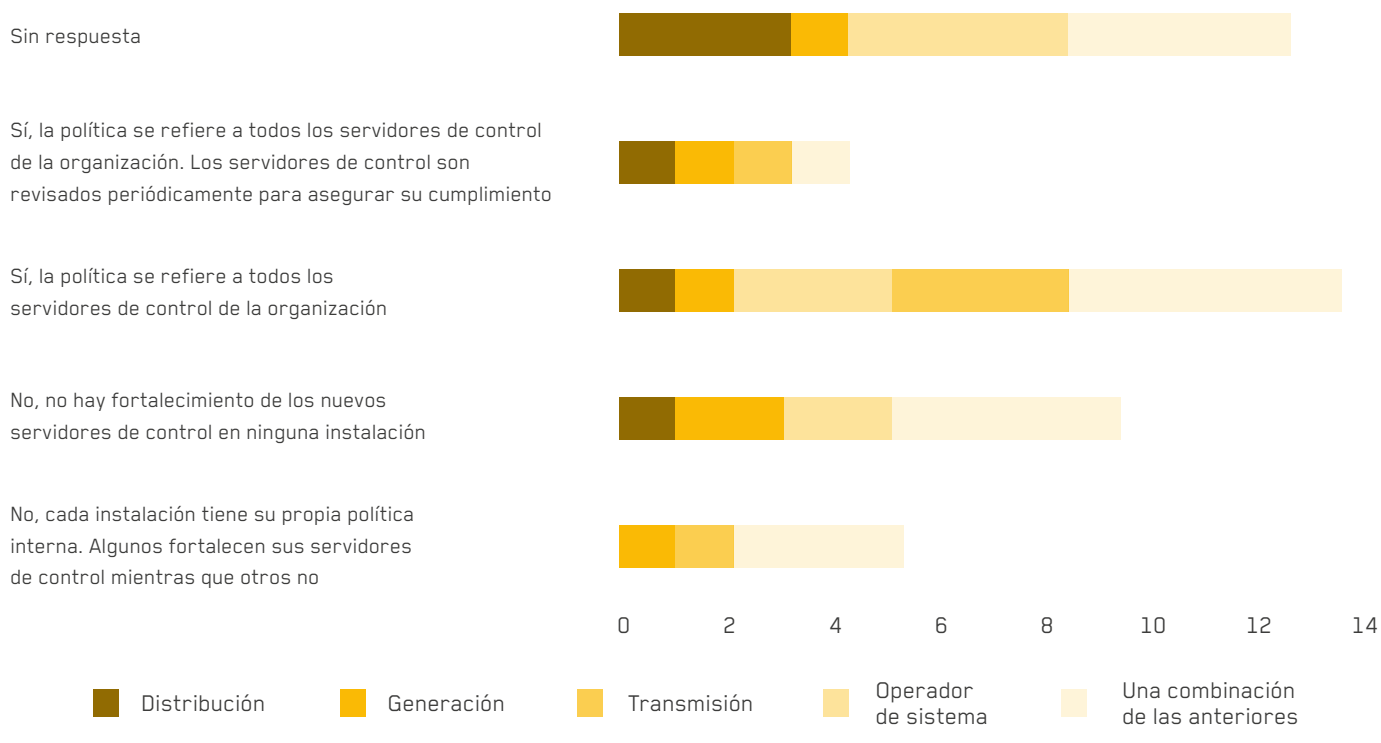


FIGURA 87. Política bastionado servidores de control.

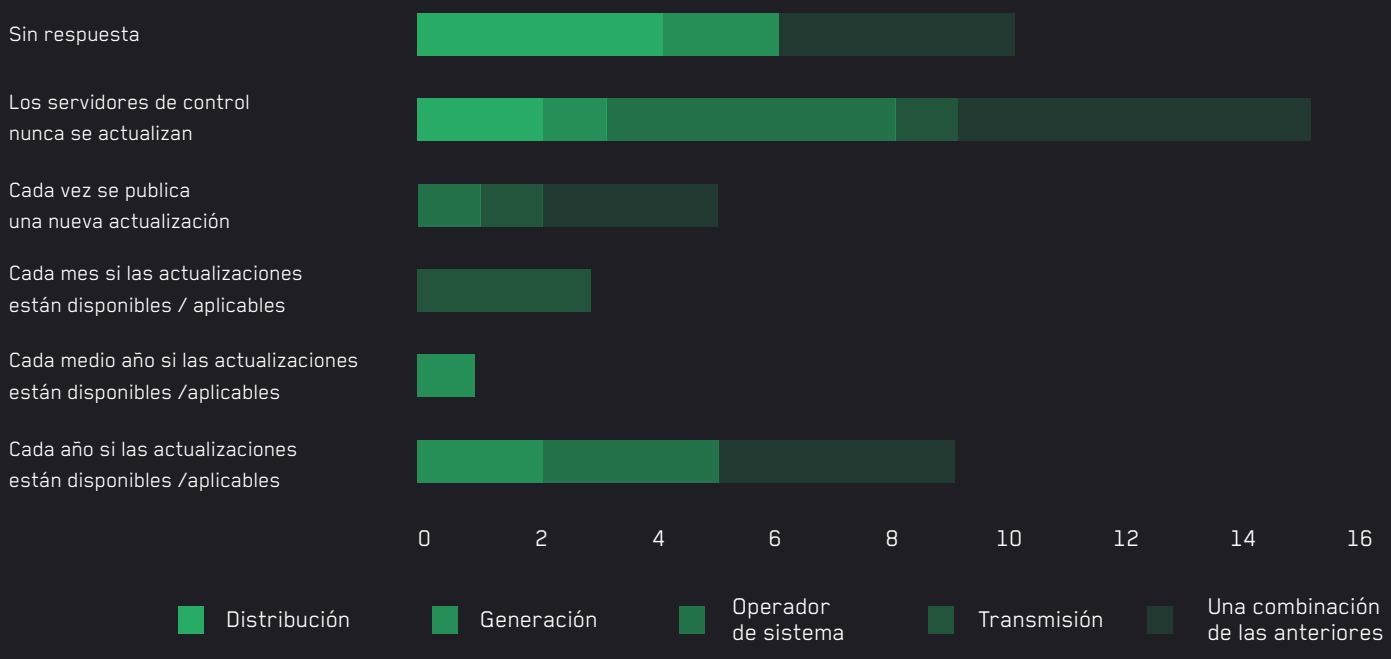


FIGURA 88. Actualización firmware servidores de control.

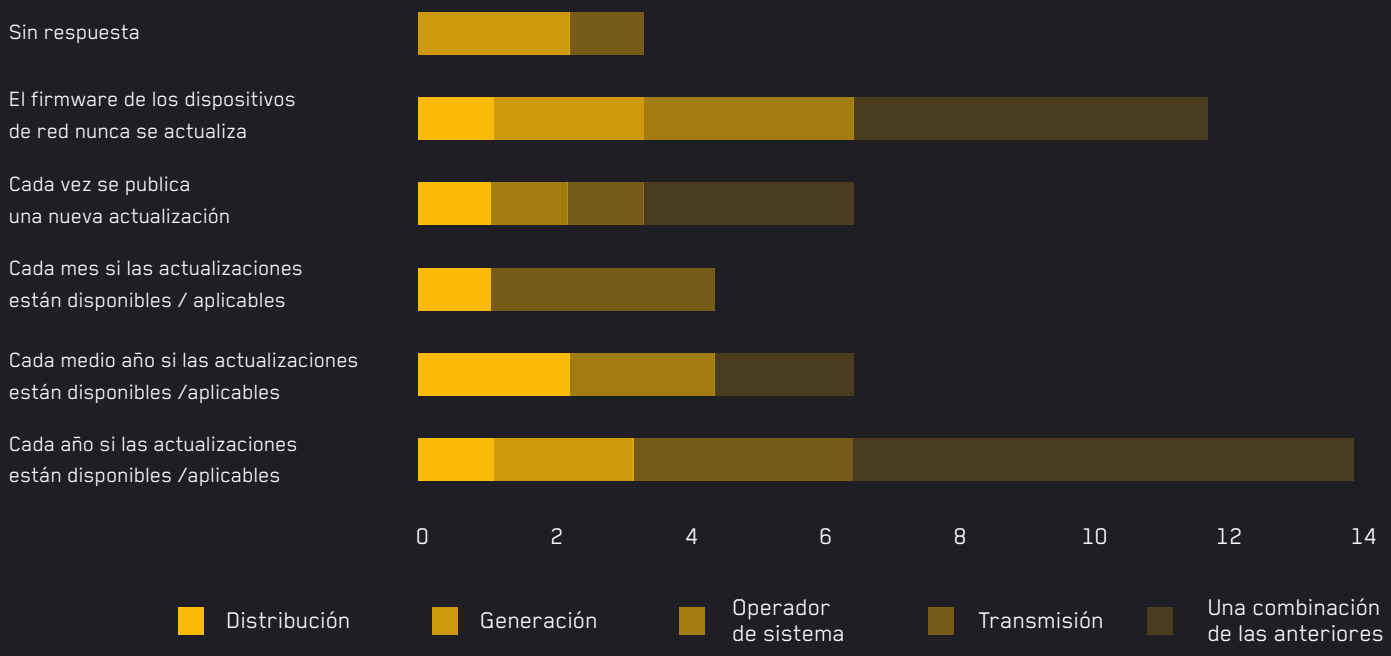


FIGURA 89. Actualización firmware de red.

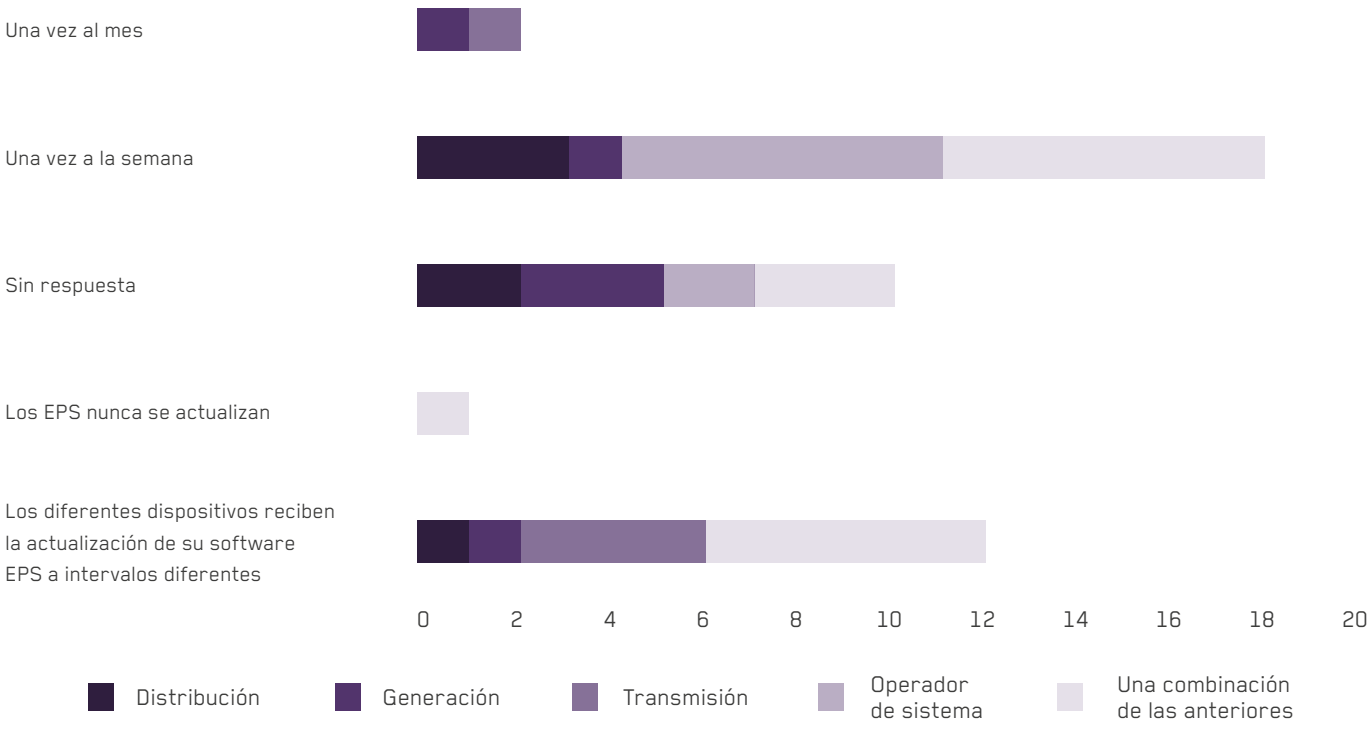


FIGURA 90. Actualización EPS.

Los equipos de red presentan un comportamiento un tanto mejor, al ser más propensos a ser actualizados. Esto se puede deber a varios factores, como: ser parte de la infraestructura TI, que su monitoreo es más especializado, o que sus vulnerabilidades son más conocidas y divulgadas.

3.4.7.5 | *Continuidad en ICS*

Para evaluar las consideraciones relacionadas con la continuidad, se revisan los aspectos considerados en la política (ver Figura 91). Aquí se examinan los escenarios que han sido considerados. El principal es recuperar ante un fallo operativo crítico, acompañado por otros escenarios donde no puedan ser operativos en un tiempo dado (MTPD), pero en último lugar quedan los ciberataques y la evaluación del plan de continuidad.

Se puede decir, casi sin excepción, que todas las empresas hacen de alguna manera copias de seguridad. Además, que estas pueden ser manuales o automatizadas, pero en varios casos de manera irregular y sin responder a unas políticas claramente definidas. (Ver Figura 92)

Se puede decir, casi **sin excepción**, que **todas las empresas** hacen de alguna manera **copias de seguridad.**

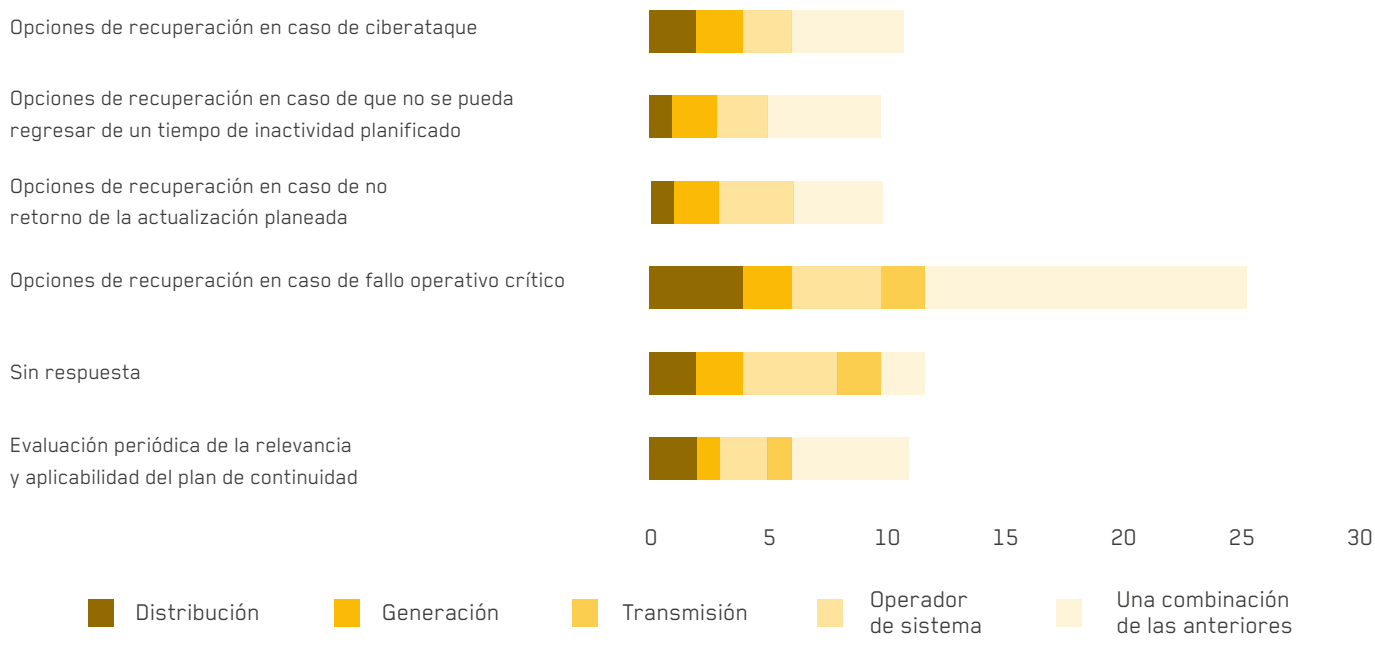


FIGURA 91. Elementos política continuidad ICS.

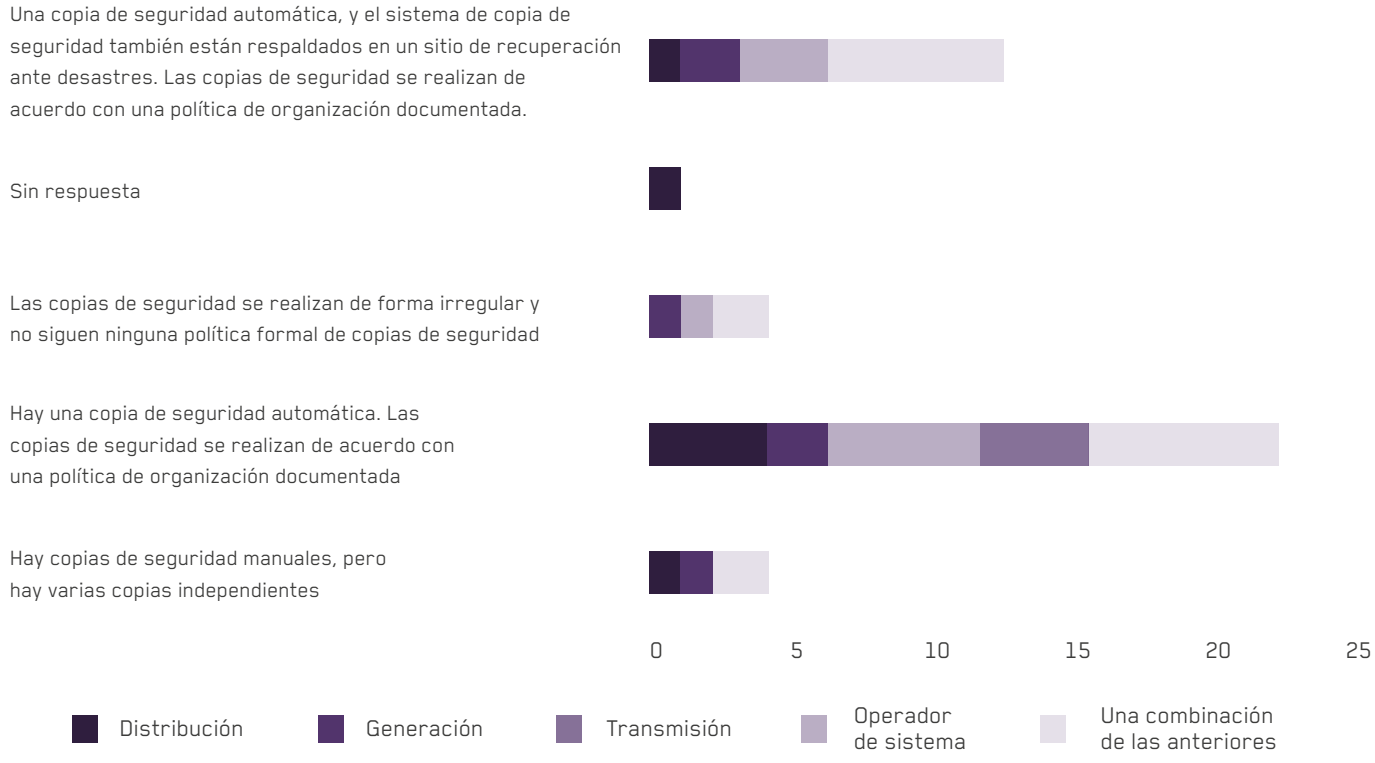


FIGURA 92. Política copias de seguridad.

Una característica común en las infraestructuras TO es el factor de redundancia en sus equipos. Esto debido a que la disponibilidad debe garantizarse sobre cualquier otro factor, puesto que una interrupción en la operación puede generar impactos económicos muy altos. Pero la red TO no siempre tiene redundancias, aunque fue reportado en menor medida en la Figura 93, también se aprecia que sí aplican buenas prácticas en el uso de redundancias de red para proteger la operación de posibles indisponibilidades generadas por la comunicación entre los componentes.

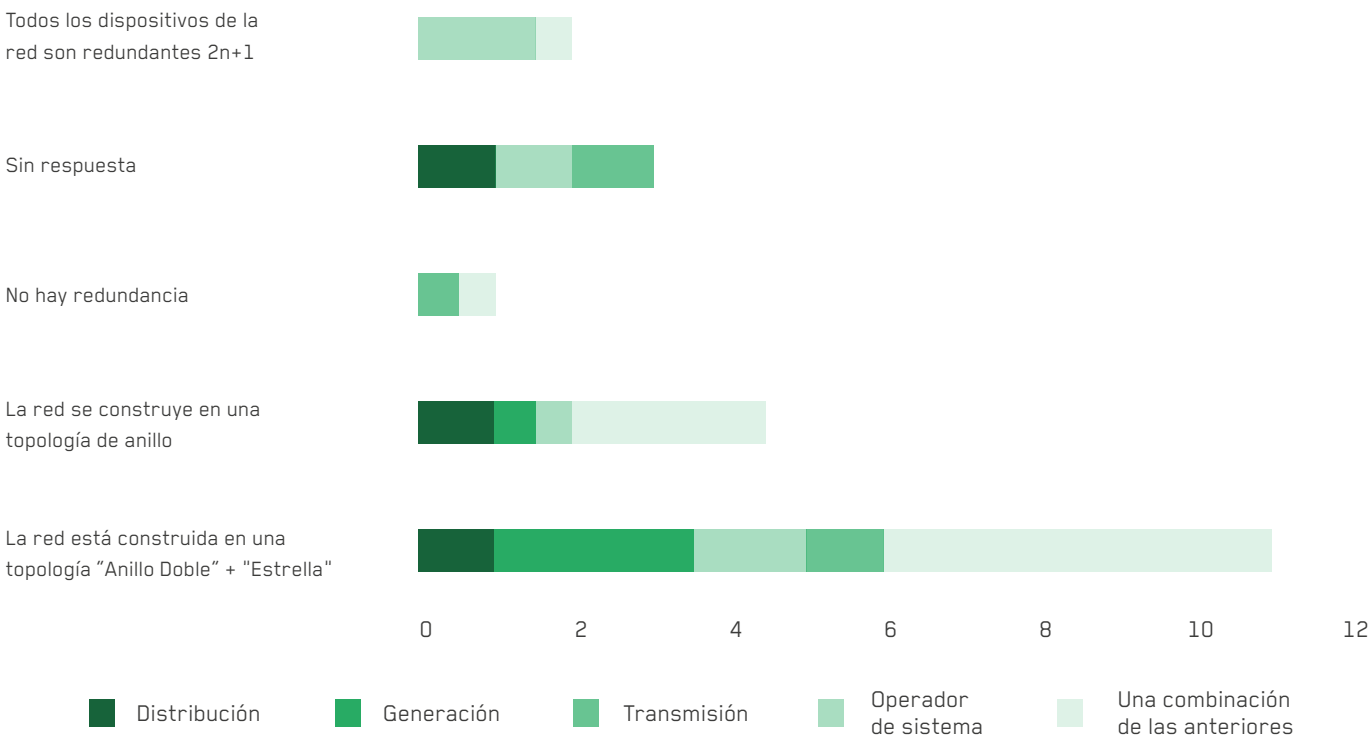


FIGURA 93. Redundancia red TO.

Finalmente, se evalúa qué tanto se respalda en las copias de seguridad. En la Figura 94 se observa como la mayoría de las veces sí hay respaldo de los archivos de configuración de los PLC. Pero en la Figura 95 se detalla la cantidad de elementos que son respaldados. Allí se incluyen:

- PLC: lógica y firmware
- Estaciones de ingeniería: aplicaciones y sistema operativo
- Servidores de control: aplicaciones y sistema operativo
- HMI: aplicaciones y sistema operativo
- Dispositivos de red: configuración y sistema operativo
- Historiadores
- Registros: dispositivos de red, de seguridad y estaciones de trabajo.

Este es un aspecto que se evidencia está muy controlado por los responsables de TO, puesto que impacta sus indicadores de rendimiento de manera directa. Es recomendable que se emplee el mismo nivel de detalle y compromiso para los demás componentes de la seguridad como son:

- Confidencialidad
- Integridad
- Autenticidad
- No repudio
- Trazabilidad
- Privacidad

De esta manera se podrá no solo garantizar una operación gobernable, sino que sea resiliente.

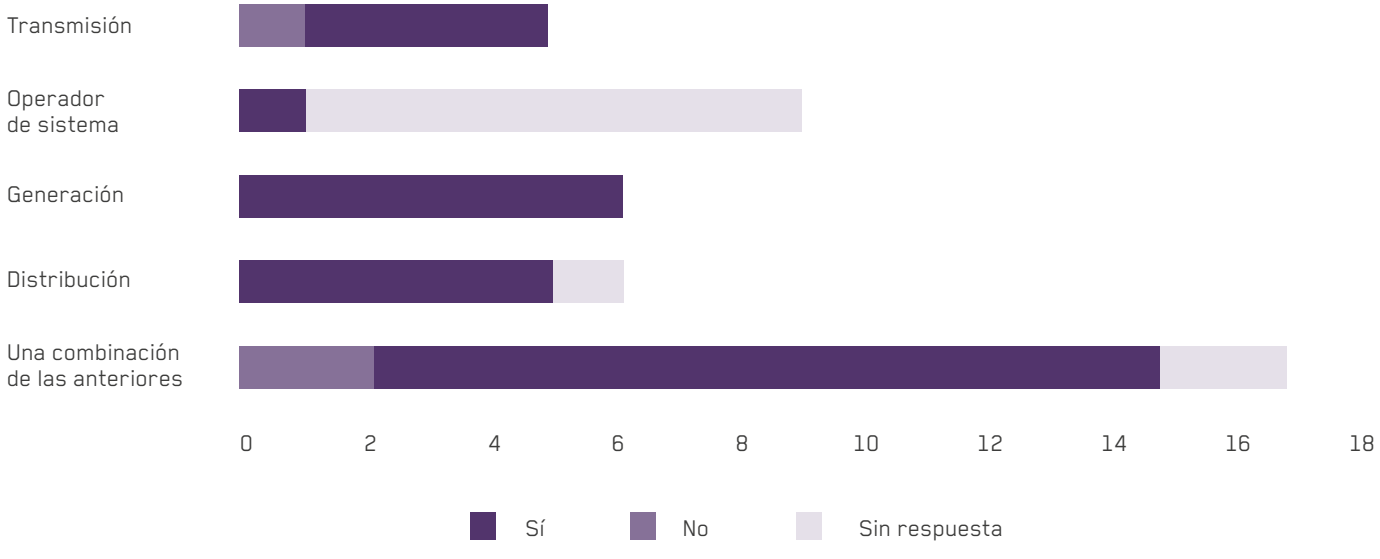


FIGURA 94. Copia de seguridad PLC.

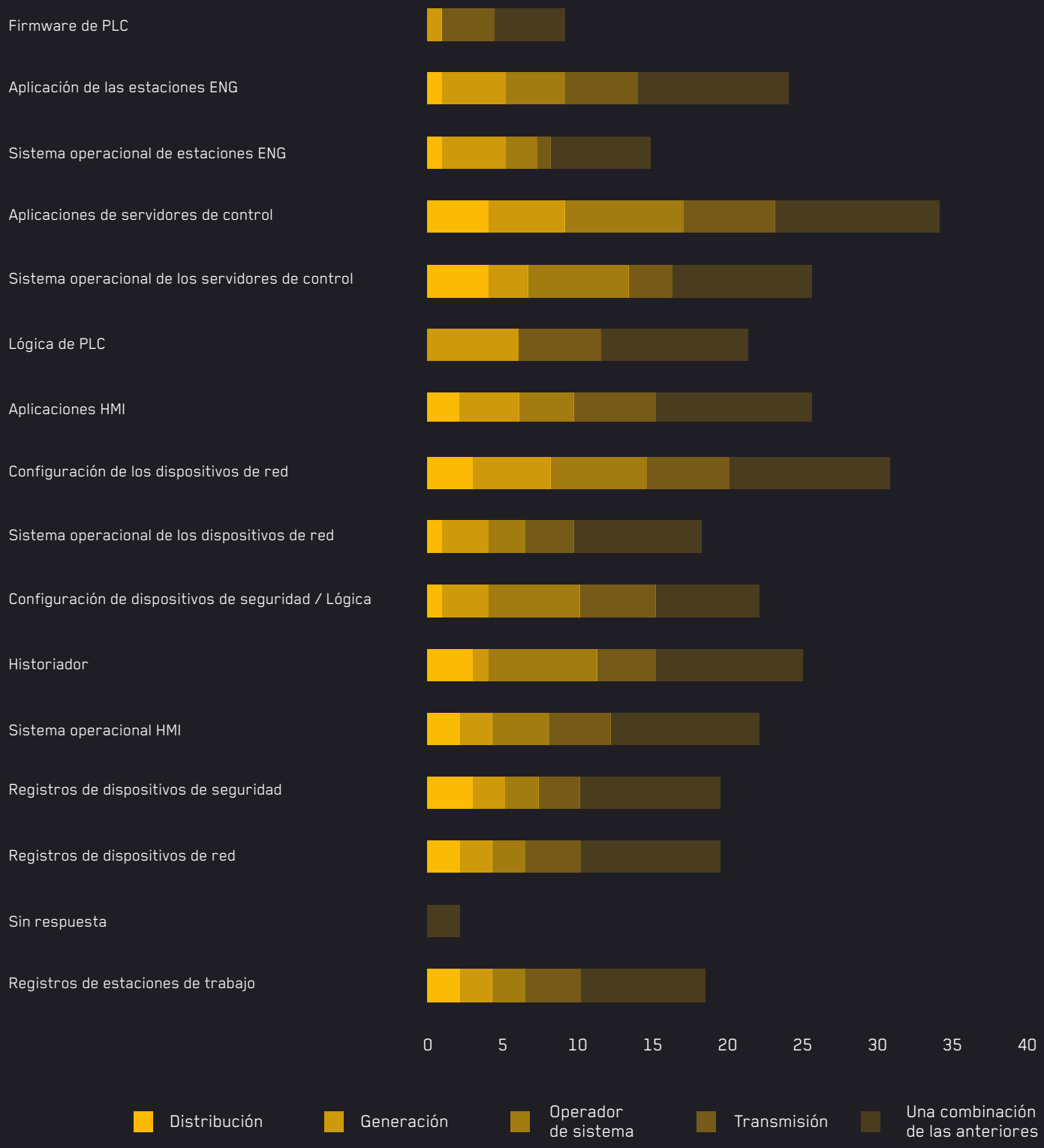


FIGURA 95. Elementos con copia de seguridad.

04

RECOMENDACIONES A FORMULADORES DE POLÍTICAS

4.1 | Consideraciones Generales

La protección de las infraestructuras de generación, transporte y distribución de energía ante posibles incidentes de ciberseguridad es una de las preocupaciones que los estados reflejan en los informes de riesgos nacionales.

El "Informe Anual de Riesgos" del Foro Económico Mundial [13] sitúa el riesgo de sufrir un ciberataque entre los cinco primeros en cuanto a probabilidad, después de los riesgos derivados de fenómenos climatológicos extremos, desastres naturales o los efectos del cambio climático. Esta tendencia ya venía mostrándose en los informes de años anteriores. En el propio informe se cita un estudio [14] que estima que **las compañías energéticas destinarán 3,2 billones de USD en 2026 para la protección de sus infraestructuras frente a ciberataques.**

La Asamblea General de la OEA, **aprobó en 2004 la Estrategia Interamericana Integral** para Combatir las Amenazas a **la Seguridad Cibernética**

Esta necesidad de protección frente a riesgos de ciberseguridad viene avalada por la catalogación, a nivel mundial, del sector energético -en general- y del subsector eléctrico -en particular- dentro del conjunto de las Infraestructuras Críticas (IICC).

En este sentido, son distintas las iniciativas reguladoras orientadas a establecer un marco normativo de protección de las infraestructuras del sector de la energía eléctrica.

La Asamblea General de la OEA, aprobó en 2004 la **Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética** [15], entre cuyos objetivos se encuentran los de establecer grupos nacionales de "alerta, vigilancia y prevención" (conocidos como CSIRT) o el de promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética. En este documento ya se alertaba sobre la posibilidad de que las amenazas cibernéticas pudieran obstaculizar las funciones de los gobiernos o interrumpir el servicio público de las infraestructuras críticas.

De los países de la OEA que ya han adoptado una Estrategia Nacional de Ciberseguridad todos ellos dedican un apartado de su Estrategia a la"Protección de Infraestructuras Críticas"donde los operadores del sector de la energía eléctrica quedarían incluidos en el denominado "catálogo de infraestructuras críticas" aunque, por el momento, algunos países todavía estén formalizando la identificación de algunas de las infraestructuras que formarían parte del catálogo. Con esta catalogación, no sólo se fortalece la seguridad de las infraestructuras críticas de cada país, sino también del sistema de infraestructuras de la región, ya que la mayor parte de ellos se encuentran interconectados.

Corresponde, una vez catalogados, ejercer las respectivas labores de control sobre el estado de la seguridad cibernética de esas infraestructuras mediante múltiples acciones que pueden incluir evaluaciones periódicas, auditoría, supervisión de funciones, formación o diseño y coordinación de ejercicios.

La Directiva europea de seguridad para las redes y sistemas de información, conocida como Directiva NIS [16], tiene entre sus objetivos el de establecer un marco común harmonizado para todos los estados miembros de la UE en lo que se refiere a los denominados Operadores de Servicios Esenciales (en los cuales se incluye el subsector eléctrico en las operaciones de generación, transporte y distribución de la energía). Uno de los objetivos de esta Directiva europea es el de instar a todos los estados miembros a que adopten una **Estrategia, entendiendo esta Estrategia Nacional de Seguridad como un marco de trabajo que provee "objetivos estratégicos y prioridades en la securización de las redes y sistemas de información en el ámbito de la nación".** Por ello, una Estrategia Nacional se convierte en un elemento clave en la protección de las infraestructuras críticas de los países.

En los Estados Unidos de América, el Departamento de Energía cuenta con su propia estrategia de ciberseguridad para la protección de las redes y sistemas federales, que se desarrolla de forma conjunta con un plan multianual de ciberseguridad en el sector energético. **La estrategia se estructura en torno a cuatro principios:**

Una **Estrategia Nacional** se convierte en un **elemento clave** en la **protección** de las **infraestructuras críticas** de los países.

1.

Alineamiento entre el Plan Estratégico del Departamento de Energía y la Estrategia de Ciberseguridad.

2.

Alineamiento entre las partes interesadas (clientes, consumidores, operadores, productores, reguladores, etc.).

3.

Alineamiento en los procesos (fomentando la creación de valor a través de la innovación, analítica de datos y *business intelligence*).

4.

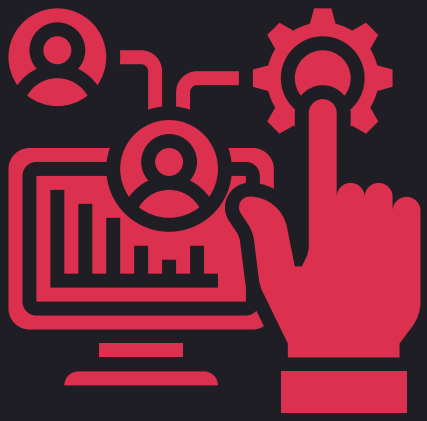
Alineamiento con la gestión del talento, involucrando a todos los recursos humanos necesarios para garantizar el éxito de la estrategia.

De forma complementaria, el Departamento de Energía ha adoptado **un modelo de madurez para ayudar a los operadores a evaluar y mejorar sus prácticas en ciberseguridad, denominado ES-C2M2 (Electricity Subsector *Cybersecurity Capability Maturity Model*).** Este marco dispone de una herramienta de autoevaluación que permite evaluar la madurez de los objetivos de cada uno de los dominios del marco:

Modelo de madurez para **ayudar a los operadores** a evaluar y mejorar sus **prácticas en ciberseguridad,** denominado **ES-C2M2** (Electricity Subsector Cybersecurity Capability Maturity Model)

- Gestión de activos
- Gestión del programa de ciberseguridad
- Gestión de la cadena de suministro y dependencias externas
- Gestión de identidad y accesos
- Continuidad de las operaciones y gestión de incidentes
- Comunicación y compartición de información
- Gestión del riesgo
- Concienciación
- Gestión de amenazas y vulnerabilidades
- Gestión de los equipos de trabajo

Basados en los antecedentes expuestos en este documento, así como en las experiencias llevadas a cabo en otras zonas geográficas como Europa o Estados Unidos, a continuación se propone un conjunto de recomendaciones para los responsables de la puesta en marcha de políticas o legislación de ciberseguridad en el sector de la energía eléctrica.



4.2 | Recomendaciones acerca del esquema de responsabilidad

Los operadores del subsector eléctrico en Latinoamérica y Caribe no son ajenos a la transformación digital que está experimentando el sector a nivel global.

Compañías de sectores diversos como el tecnológico, financiero, logístico, etc. están incorporando nuevos escenarios en sus estrategias digitales, como son el *Cloud Computing* (computación en la nube) o el *Big Data* (análisis de datos a gran escala).

Estas tecnologías pueden ser requeridas para la mejora de la competitividad de las compañías eléctricas, en especial, con el impulso de las redes "Smart" [17]. La definición del *European Smart Grid Task Force* indica que **las redes *Smart Grid* son aquellas "redes eléctricas que pueden integrar con eficiencia los comportamientos y acciones de todos los usuarios conectados a ella – generadores, consumidores y los que juegan ambos roles – con el objetivo de asegurar un sistema energético económicamente eficiente, sostenible, con bajas pérdidas y altos niveles de calidad y seguridad en el suministro".**

Todos los implicados en el mercado energético, tanto del sector público como privado, deben ser conscientes de los riesgos de ciberseguridad que introducen estas nuevas tecnologías, para lo cual es necesario establecer un marco regulatorio común en la región.

Las recomendaciones para desarrollar un marco común de seguridad incluyen:

1.

Identificación de las infraestructuras críticas y de los operadores de infraestructuras críticas

Los estados deben desarrollar las Estrategias Nacionales de Ciberseguridad, siguiendo la hoja de ruta marcada por la OEA, en las cuáles deben incluir la definición de Infraestructuras Críticas estableciendo los adecuados criterios de clasificación. Se identificarán los sectores y subsectores considerados como críticos para el país y se establecerá un mecanismo de designación de operadores críticos. Estos operadores, ya sean públicos o privados, deberán disponer de sus planes de protección en ciberseguridad, identificando amenazas y vulnerabilidades en sus infraestructuras, los cuales serán revisados por el organismo competente en la materia con el fin de que estén alineados con los requerimientos de la Estrategia Nacional.

2.

Desarrollo de una Estrategia de seguridad del sector energético

Los gobiernos deben impulsar el desarrollo de normativas (en forma de marcos, guías, recomendaciones, etc.) para dotar al sector energético de un mayor nivel de madurez en cuanto a ciberseguridad. Estos marcos deben considerar los elementos de gestión y evaluación del riesgo como una de las piezas clave de su estrategia. Una eficaz evaluación del riesgo permitirá establecer los controles adecuados para garantizar la seguridad de un sistema, y permitirá su evolución frente a la adopción de nuevas tecnologías en el sector: *Cloud Computing*, *Big Data* o *Smart Grid*.

El marco sectorial resultante debe contemplar estrategias de **ciber resiliencia** para asegurar la continuidad del servicio en caso de un incidente de seguridad, tanto si el incidente tiene su origen en un ataque cibernético como si es debido a fallos humanos, accidentes fortuitos o desastres naturales.

Para alcanzar los objetivos de las estrategias de ciberseguridad, se establecerán autoridades relevantes con la misión de coordinar la estrategia en el sector y de establecer estándares para el adecuado manejo de ciberriesgos en los operadores, así como desarrollar los cuerpos regulatorios oportunos que definan los roles y responsabilidades tanto del sector público como privado e identifiquen las áreas clave donde la reducción del riesgo se torne prioritaria.

3.

Colaboración nacional e internacional

La interconexión de las distintas redes de transporte de energía eléctrica puede traspasar los límites fronterizos entre países. Esta situación motiva que sea necesario establecer mecanismos de comunicación y cooperación a nivel internacional a efectos de prevención, identificación, respuesta y recuperación de incidentes de ciberseguridad en la red o los operadores eléctricos. Un incidente de seguridad cibernética en la red eléctrica puede afectar a varios países, por lo que se debe contar con procedimientos para la gestión de crisis o recuperación ante desastres que sean aplicables en un contexto interestatal.

El marco colaborativo puede verse reforzado con la promoción de encuentros sectoriales periódicos, o la creación de foros donde participen todas las partes implicadas de la industria de la energía eléctrica. Estos foros, ya sean de ámbito nacional o internacional, deben permitir compartir el conocimiento, identificar nuevas ciberamenazas y revisar los ciberataques ocurridos para extraer conclusiones y lecciones aprendidas.

4.

Coordinación de acciones: Equipo de respuesta a incidentes

La adopción de medidas individuales por parte de los operadores eléctricos, ya sean públicos o privados, puede resolver necesidades a corto, medio o largo plazo del operador, pero no contribuye a garantizar la seguridad de la red eléctrica de un país si las mencionadas medidas no van acompañadas de una estrategia común de protección de las infraestructuras críticas. Por ello es imprescindible la existencia de un marco común de cooperación y de intercambio de información entre las partes involucradas y las autoridades públicas.

La cooperación y coordinación entre las partes interesadas permitirá detectar y gestionar un incidente en el instante en que se origina (o en intervalo de tiempo muy próximo al momento inicial), permitiendo así reducir su impacto y su alcance. Para ello se debería contar con sistemas de Alerta Temprana, capaces de detectar un incidente de forma rápida y de detectar anomalías dentro de la red. Estos sistemas deben permitir la monitorización del tráfico en tiempo real para proceder a su análisis y correlación por parte de los organismos competentes.

Gracias a las capacidades de los mecanismos de alerta temprana y al intercambio fluido de información, se podrá coordinar una respuesta desde los centros de respuesta a incidentes (CSIRT, por sus siglas en inglés). Los CSIRT serán los encargados de coordinar la respuesta, recuperación y reporte de incidentes de ciberseguridad para el sector.

Estas recomendaciones **deben** ser abordadas por los **gobiernos y** reflejadas en sus **respectivas estrategias** nacionales de ciberseguridad, **siendo los** encargados de **establecer autoridades** relevantes y los **organismos** de **control,** como serían **-por ejemplo- un centro** nacional para la protección de las infraestructuras **críticas o un CSIRT para el** sector energético.

4.3 Recomendaciones acerca de los roles de la academia, la educación pública y el sector privado

En el apartado anterior se destacó la responsabilidad de los gobiernos y de las instituciones públicas en la protección del subsector eléctrico frente a incidentes de seguridad así como de las infraestructuras críticas asociados. No obstante, otras partes interesadas también son cruciales para el éxito de la ciberprotección del sector.

La cultura de la seguridad es una de las piezas clave, que debe venir respaldada por campañas de formación y concienciación en la materia, ya que los usuarios que operan, diseñan, mantienen o –simplemente- tienen acceso a los sistemas de control y automatización de las redes eléctricas deben conocer los riesgos de ciberseguridad a los que estos sistemas pueden estar expuestos.

Se debe fomentar la formación en seguridad en los planes de formación del sector (técnicos, instaladores, supervisores, personal de mantenimiento, ingenieros, etc.), así como desarrollar planes específicos para formar a profesionales de la ciberseguridad en los sistemas de TO contemplando tanto la creación de planes de estudios regulados como mediante certificaciones profesionales.

La capacitación y las certificaciones **deben incluir** los siguientes **elementos:**

1.

Comprender el proceso operativo, los riesgos operativos y las limitaciones.

2.

Comprensión de los principales ciberataques de TO y sus consecuencias.

3.

Análisis de ciberataques ocurridos.

4.

Comprender el proceso de evaluación del riesgo en TO.

5.

Definición y diseño de políticas y procedimientos de seguridad cibernética de TO.

6.

Gestión de incidentes cibernéticos TO (primer, segundo y tercer nivel).

7.

Herramientas y soluciones de protección cibernética TO.

8.

Diseño y mantenimiento de planes de Continuidad de negocio y planes de recuperación ante desastres (DRP).

9.

Concienciación en seguridad TO y actualizaciones de amenazas.

10.

Capacitación profesional para respuesta a incidentes de TO.

11.

Los empleados que operan y administran soluciones de protección cibernética deben estar certificados de acuerdo con los requisitos del fabricante.

Finalmente, se debe impulsar la investigación y desarrollo de sistemas de suministro de energía con capacidades de ciber resiliencia incorporadas, lo que requiere planes de impulso sectoriales soportados con ayudas e inversión pública, máxime teniendo en cuenta que muchos esfuerzos de investigación y desarrollo no son justificables desde el punto de vista del sector privado.

4.4 | Hoja de ruta

4.4.1 | META A: definir un marco regulatorio para la protección de infraestructuras críticas del subsector eléctrico

A **DEFINIR UN MARCO REGULATORIO PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS DEL SECTOR ENERGÉTICO**

1 **Establecer estructuras definidas para la ciberseguridad industrial**

- **A.1.1.** Definir Autoridades competentes
- **A.1.2.** Definir CSIRTs de referencia
- **A.1.3**. Definir un Consejo de Ciberseguridad Nacional

2 **Elaborar directrices legales que sustenten el marco regulatorio**

- **A.1.1.** Obligar legalmente a la notificación de incidentes
- **A.1.2.** Disponer de un registro actualizado de Infraestructuras Críticas del subsector eléctrico
- **A.1.3.** Establecer un régimen sancionador

FIGURA 96. Meta A: Definir un marco regulatorio para la protección de Infraestructuras críticas del subsector eléctrico.

4.4.1.1 | Objetivo

A.1. Establecer estructuras definidas e independientes para las diferentes funciones necesarias para dar cumplimiento al marco regulatorio

4.4.1.1.1 | ACCIÓN A.1.1.

Definir Autoridades Competentes

Designar, tanto para el sector privado como público, un organismo encargado de la supervisión, vigilancia y sanción y que verifiquen el cumplimiento de la normativa sectorial y la adopción de las medidas de seguridad que sean precisas en cada plan de protección.

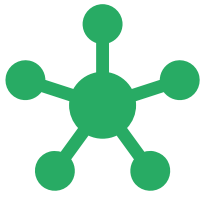
4.4.1.1.2 | ACCIÓN A.1.2.

Definir CSIRTs de referencia

La conducción operativa de respuesta a incidentes, de forma que se pueda realizar una adecuada gestión (ver segunda Meta), es una actividad crucial en la protección de infraestructuras críticas, por lo que debe designarse legalmente un organismo encargado para cada sector.

4.4.1.1.3 | ACCIÓN A.1.3.

Definir Consejo de Seguridad Nacional



Se necesita un organismo que coordine las relaciones de coordinación, colaboración y cooperación entre los diferentes sectores y órganos de la administración en materia de ciberseguridad.

4.4.1.2 | Objetivo

A.2. Elaborar directrices legales que sustenten el marco regulatorio

4.4.1.2.1 | ACCIÓN A.2.1.

Obligar legalmente a la notificación de incidentes de manera anónima

En el caso de una contingencia con efectos sobre una infraestructura crítica de tipo energético, los efectos pueden acarrear muchas consecuencias; por ello, la notificación de incidentes debe ser obligatoria.

4.4.1.2.2 | ACCIÓN A.2.2.

Disponer de un registro actualizado de Infraestructuras Críticas del subsector eléctrico

La conducción operativa de respuesta a incidentes, de forma que se pueda realizar una adecuada gestión (ver segunda Meta), es una actividad crucial en la protección de infraestructuras críticas, por lo que debe designarse legalmente un organismo encargado para cada sector.

4.4.1.2.3 | ACCIÓN A.2.3.

Establecer un régimen sancionador

Debe penalizarse el incumplimiento del marco de protección, sobre todo en lo referido a notificación de incidentes y no implementación de los controles, de forma que los operadores se impliquen en la implantación de las medidas necesarias.

4.4.2 META B: Robustecer la estrategia de seguridad del sector energético aumentando su preparación ante ciberamenazas

B ROBUSTECER LA ESTRATEGIA DE SEGURIDAD DEL SECTOR AUMENTANDO SU PREPARACIÓN ANTE CIBERAMENAZAS

1 Entendimiento del entorno en cuanto a ciberseguridad

B.1.1. Establecer e impulsar canales y procedimientos para el flujo de información relativa a seguridad desde y hacia los operadores

B.1.2. Explorar maneras de abrir canales para coordinarse con otras naciones en la preparación ante amenazas de ciberseguridad industrial

B.1.3. Impulsar una oficina de inteligencia-contrainteligencia con actividad en la detección de amenazas del sector energético

2 Herramientas para compartir información

B.2.1. Establecer una plataforma que recolecte automáticamente información IT y OT desde las redes de los operadores y la envíe en forma encriptada a un centro de análisis

B.2.2. Desarollar una plataforma colaborativa virtual de investigación y análisis de malware

FIGURA 97. Meta B: Robustecer la estrategia de seguridad del sector energético aumentando su preparación ante ciberamenaza.

3 Mejora de gobierno y gestión de riesgos

B.3.1. Fortalecer la capacidad de toma de desiciones fundamentada de los Departamentos o Ministerios de Energía para la protección de las infraestructuras energéticas

B.3.2. Implantar recursos técnicos que faciliten la labor de análisis de riegos y monitorización

B.3.3. Implantar recursos que faciliten la labor de mitigación y control de riesgos

B.3.4. Establecer estructuras de certificación de seguridad para productos y servicios a nivel de industrial

4 Recuperación y restuauración

B.4.1. Asistirle en el desarrollo de Planes de Recuperación y Restauración validados para las infraestructuras más críticas de cada operador

B.4.2. Establecer mecanismos para la orquestación de planes de recuperación de múltiples actores simultáneos del sector energético

4.4.2.1 | Objetivo

B.1.

Conseguir un entendimiento efectivo del entorno y situación del sector desde el punto de vista de la ciberseguridad

4.4.2.1.1 ACCIÓN B.1.1.

Establecer e impulsar canales y procedimientos para el flujo de información relativa a seguridad desde y hacia los operadores

Se debe favorecer la comunicación relevante y oportuna de la situación respecto de la ciberseguridad, especialmente entre el sector privado y público, creando un espacio de confianza mutua y colaboración, mediante el soporte de canales y procedimientos bajo la dirección del Departamento o Ministerio de Energía.

Además, se debe desarrollar e implementar un proceso iterativo donde se solicite información sobre requerimientos de operadores en cuanto a seguridad, sin penalizarles por dicho reporte de necesidades, de forma que más tarde puedan proveerse los servicios o soportes necesarios en la materia.

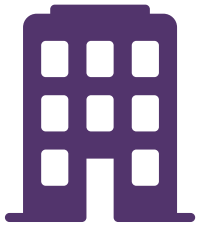
4.4.2.1.2 ACCIÓN B.1.2.

Explorar maneras de abrir canales para coordinarse con otras naciones en la preparación ante amenazas de ciberseguridad industrial

En los ataques a gran escala puede ser muy eficaz la compartición de información con otros socios comerciales o de la región. Por tanto, el Departamento o Ministerio de Energía, en colaboración con la Administración Pública, explorará vías para el desarrollo de sistemas que intercambien información relevante y permita la coordinación frente a las potenciales ciberamenazas de alcance global.

4.4.2.1.3 | ACCIÓN B.1.3.

Impulsar una oficina de inteligencia-contrainteligencia con actividad en la detección de amenazas del sector energético



Esta entidad, creada por el Departamento o Ministerio de Energía, deberá investigar y proveer a los operadores del sector de información sobre ciberamenazas emergentes. De esta forma, debería identificar y cuantificar los más recientes ciberataques para comunicarlo a las partes interesadas, y compartir información con los agentes de inteligencia locales/nacionales oportunos. Así, será posible detectar a tiempo posibles ataques coordinados y/o dirigidos y establecer medidas adecuadas.

4.4.2.2 | Objetivo

B.2.

Impulsar la implantación de herramientas para compartir información entre los diferentes actores

4.4.2.2.1 | ACCIÓN B.2.1.

Establecer una plataforma que recolecte automáticamente información TI y TO desde las redes de los operadores y la envíe en forma encriptada a un centro de análisis

Los Departamentos o Ministerios de Energía impulsarán una plataforma donde analizar eventos de diferentes fuentes dentro del sector y podrán, a través de su correlación, generar información de contrainteligencia que permitirá determinar medidas de mitigación acerca de potenciales amenazas dañinas y comunicarlas en tiempo real a los operadores.

4.4.2.2.2 | ACCIÓN B.2.2.

Desarrollar una plataforma colaborativa virtual de investigación y análisis de malware

En este tipo de plataforma, impulsada también por los Departamentos o Ministerios de Energía, se podrán realizar pruebas de programas, código o sitios web desconocidos o de fuentes no confiables, sin arriesgarse a dañar los dispositivos físicos reales. Mediante su investigación y análisis se podrá diseñar un catálogo de potenciales elementos y fuentes maliciosas.

4.4.2.3 | Objetivo

B.3. Mejorar el gobierno y gestión del riesgo tecnológico en todos los agentes del sector

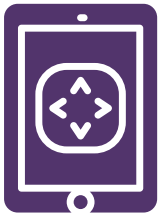
4.4.2.3.1 | ACCIÓN B.3.1.

Fortalecer la capacidad de toma de decisiones fundamentada de los Departamentos o Ministerios de Energía para la protección de las infraestructuras energéticas

Revisar, mejorar y formalizar sus procesos de gobierno y dotarlos de un enfoque de gestión basado en riesgos. Para ello, se deberán implementar métricas para monitorizar y analizar el riesgo y la efectividad de las medidas de su mitigación.

4.4.2.3.2 ACCIÓN B.3.2.

Implantar recursos técnicos que faciliten la labor de análisis de riesgos y monitorización



Los Departamentos o Ministerios de Energía deberán desarrollar y/o promover herramientas para la realización de análisis de riesgos y la automatización de respuestas, así como la monitorización continua de sistemas; de forma que se reduzca la complejidad y coste de estas funciones. De forma paralela, proveer de guías, entrenamiento y asistencia técnica a los operadores, de manera que sus capacidades de manejo de ciberriesgos se vean fortalecidas.

4.4.2.3.3 ACCIÓN B.3.3.

Implantar recursos que faciliten la labor de mitigación y control de riesgos

Se deberán desarrollar políticas que dirijan el establecimiento de la ciberhigiene mediante el uso de herramientas automáticas, el fortalecimiento de controles internos y la estandarización de procesos para agilizar el proceso de mitigación y control de riesgos.

4.4.2.3.4 ACCIÓN B.3.4.

Establecer estructuras de certificación de seguridad para productos y servicios a nivel de industria

Estas certificaciones, validadas por el Departamento o Ministerio de Energía, permitirán asegurar que los productos y servicios cumplen con los estándares de ciberseguridad requeridos y se adaptan a las rápidas evoluciones del mercado y a la aparición de nuevas amenazas, mediante la diferenciación de dichos productos y servicios basándose en sus cualidades de seguridad.

4.4.2.4 | Objetivo

B.4. Disponer de Planes de Recuperación de Desastres y Restauración sobre las infraestructuras más críticas de los distintos agentes del sector

4.4.2.4.1 ACCIÓN B.4.1.

Asistir en el desarrollo de Planes de Recuperación y Restauración validados para las infraestructuras más críticas de cada operador

Los operadores deberán estar preparados en el caso de eventos que supongan una interrupción o grave perturbación de sus servicios, por lo que se necesitará apoyarse sobre una infraestructura TI y TO robusta, confiable y redundada. Para ello debe realizarse un análisis diferencial previo de recursos TI y TO necesarios para acometer dichos planes de recuperación y prestar servicios de continuidad, así como una identificación de los servicios más críticos y que deben recuperarse en primer lugar.

4.4.2.4.2 ACCIÓN B.4.2.

Establecer mecanismos para la orquestación de planes de recuperación de desastres de carácter sectorial

Para asegurar en el mayor grado posible que el impacto de un ciber ataque sobre uno o varios operadores (en el peor caso, provocando una interrupción del servicio) pueda mitigarse eficazmente, los Departamentos o Ministerios de Energía deberán diseñar una estructura organizada mediante la que puedan articular una respuesta de carácter sectorial en el caso de eventos disruptivos, de forma que se pueda seguir ofreciendo unos niveles de suministro adecuados a los ciudadanos.

4.4.3 | META C: Coordinar la respuesta, recuperación y reporte de incidentes de ciberseguridad a lo largo del sector de manera eficaz

C COORDINAR LA RESPUESTA, RECUPERACIÓN Y REPORTE DE CIBER-INCIDENTES EN EL SECTOR ENERGÉTICO

1 Estructuras competentes para la respuesta en entornos industriales

C.1.1. Impulsar la coordinación y respuestas a eventos de seguridad a través de un CSIRT especializado en tecnologías industriales

C.1.2. Establecer procesos coordinados de respuesta

2 Sistema de reporte de ciberseguridad

C.2.1. Definir o actualizar los procesos de respuesta ante ciber-incidentes

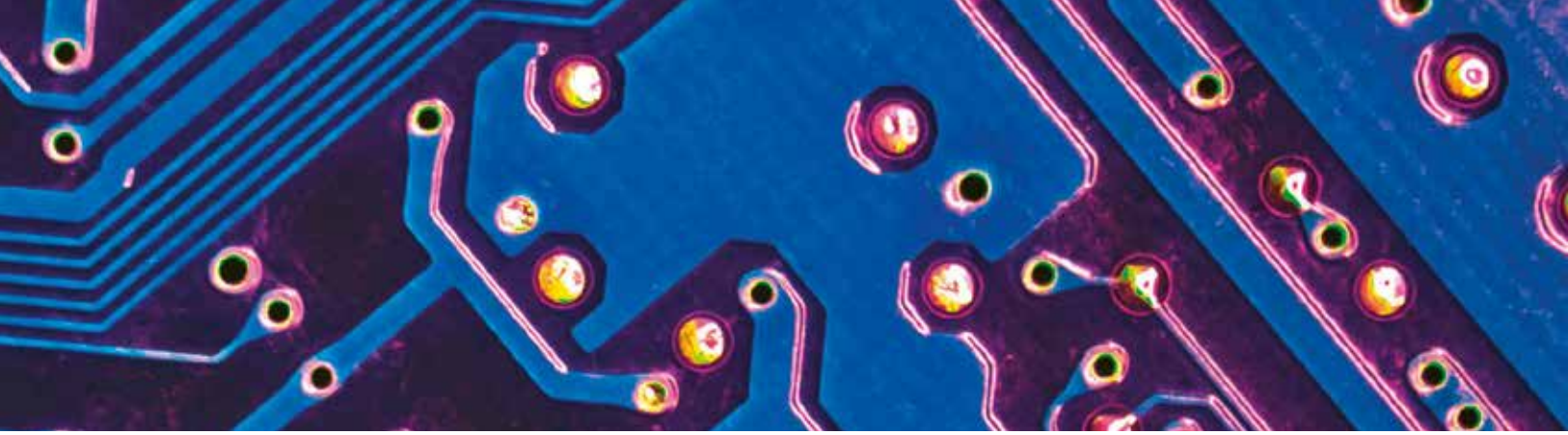
C.2.2. Desarrollar y proveer entrenamiento especializado en respuesta a ciber-incidentes

3 Realización de ejercicios de simlulación

C.3.1. Realizar simulaciones coordinadas de detencción y respuesta, incluyendo la recuperación y restauración de los servicios

C.3.2. Desarrollar competiciones donde se valide el conocimiento y las habilidades de los expertos actuales y futuros en ciberseguridad

FIGURA 98. Meta C: Coordinar la respuesta, recuperación y reporte de incidentes de ciberseguridad a lo largo del sector de manera eficaz.



4.4.3.1 | Objetivo

C.1.

Establecer una estructura competente para la respuesta ante ciber incidentes a escala nacional en el sector energético

4.4.3.1.1 ACCIÓN C.1.1.

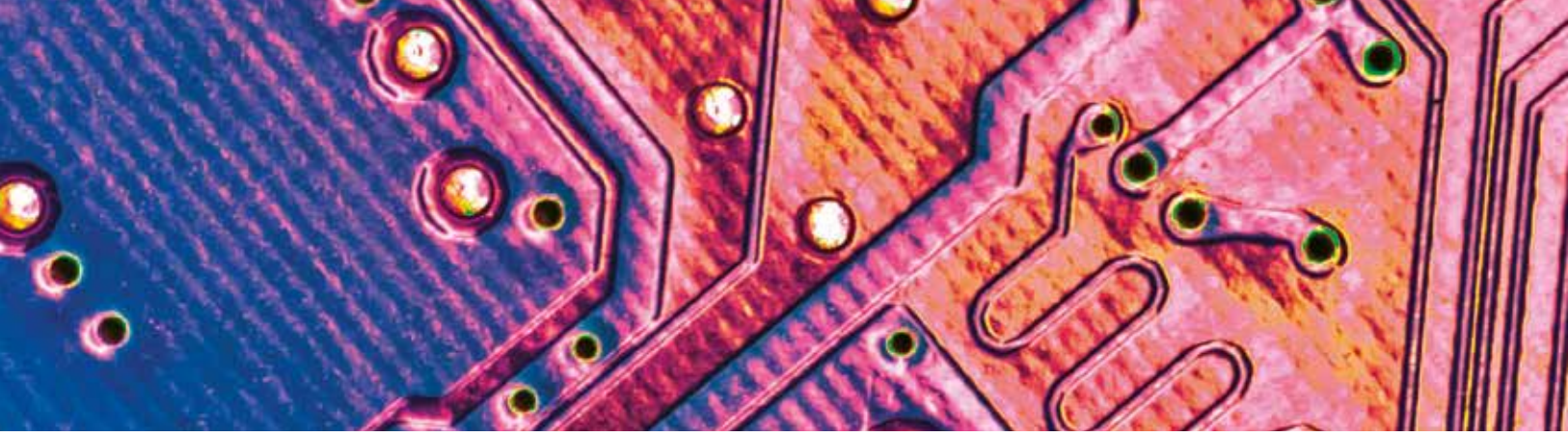
Impulsar la coordinación y respuesta a eventos de seguridad a través de un CSIRT especializado en tecnologías industriales

El Departamento o Ministerio de Energía debería impulsar un CISRT para coordinar y dar respuesta en tiempo real a las posibles amenazas que se materialicen en los operadores.

4.4.3.1.2 ACCIÓN B.4.2.

Establecer procesos coordinados en materia de respuesta ante ciber-incidentes

Los Ministerios o Departamentos de Energía deben crear o actualizar sus procesos internos de coordinación de mecanismos para la resolución de ciber incidentes que incluyan formatos comunes del reporte de incidentes, asegurando también su coordinación con operadores privados de forma que estos sigan las mismas pautas.



4.4.3.2 | Objetivo

C.2. Establecer un sistema de reporte y entrenar a los actores en la respuesta ante ciber incidentes

4.4.3.2.1 | ACCIÓN C.2.1.

Definir o actualizar los procesos de reporte de incidentes

El reporte a tiempo de ciber incidentes o eventos de seguridad es fundamental para una respuesta efectiva, así como la correlación de eventos en distintas ubicaciones que permitan identificar ataques coordinados, la identificación de los perpetradores de los mismos y la prevención de futuros incidentes. Por ello, es importante que los Ministerios de Energía fomenten el reporte de incidentes en tiempo real desde los operadores.

4.4.3.2.2 | ACCIÓN C.2.2.

Desarrollar y proveer formación y entrenamiento en respuesta ante ciber-incidentes

Los Departamentos o Ministerios de Energía deben elaborar planes de formación y entrenamiento que incluyan información sobre ciber ataques y cómo actuar cuando se produzcan, así como los recursos que pueden prestar a los operadores.

4.4.3.2 | Objetivo

C.3.

Realizar ejercicios de simulación de la capacidad de respuesta ante incidentes por parte de todos los operadores implicados

4.4.3.3.1 ACCIÓN C.3.1.

Realizar simulaciones coordinadas de detección y respuesta de ciber-incidentes, incluyendo acciones de recuperación y restauración de los servicios

Se realizarán pruebas periódicas implicando a autoridades locales y operadores para probar sus capacidades de coordinación y respuesta, de forma que se identifiquen aspectos de mejora en cuanto a regulación y procedimientos en el sector. Estas simulaciones podrán tener carácter de desastre y medirán la capacidad de respuesta de la nación ante una disrupción grave en el sector energético.

4.4.3.3.2 ACCIÓN C.3.2.

Desarrollar competiciones donde se valide el conocimiento y las habilidades de los expertos actuales y futuros en ciberseguridad

En estas competiciones se medirán los talentos actuales y de los estudiantes que pueden constituirse en futuros expertos de la seguridad en el sector energético, se perseguirá atraer el interés de estudiantes de carreras en ciberseguridad sobre los sistemas industriales en general y del sector energético en particular, permitiendo ponerse a prueba sobre entornos y sistemas reales o simulados.

4.4.4 | META B: Fomentar la investigación, desarrollo, innovación y certificación de componentes y sistemas ciberresilientes

D INVESTIGACIÓN, DESARROLLO, INNOVACIÓN
Y CERTIFICACIÓN DE COMPONENTES Y SISTEMAS CIBERRESILIENTES

1 Tecnologías para la prevención, detección y mitigación de ciberincidentes

- **D.1.1.** Impulsar el desarrollo de herramientas para la prevención y detección de ciberincidentes que evolucionen de acuerdo con el entorno de amenazas cambiante
- **D.1.2** Impulsar sistemas que protejan la información confidencial de seguridad en las Infraestructuras Críticas del sector

2 Mejora continua de la seguridad en los sistemas de la infraestructura del sector

- **D.2.1.** Aportar incentivos para la innovación en seguridad mediante la protección de derechos de propiedad intelectual
- **D.2.2.** Respaldar la adopción de estrategias de benchmarking de ciberseguridad
- **D.2.3** Reconocer la excelencia profesional en el ámbito de la ciberseguridad

FIGURA 99. Meta B: Robustecer la estrategia de seguridad del sector energético aumentando su preparación ante ciberamenazas.

4.4.4.1 | Objetivo

D.1.

Investigar, desarrollar herramientas y tecnologías para la prevención, detección y mitigación de ciberincidentes en el sector energético

4.4.4.1.1 ACCIÓN D.1.1.

Impulsar el desarrollo de herramientas para la prevención y detección de ciberincidentes que evolucionen de acuerdo con el entorno de amenazas cambiante

Los Departamentos o Ministerios de Energía deben promover el desarrollo de herramientas con un enfoque específico sobre el entorno de TO y que incorporen la información sobre las amenazas más actuales o de última tendencia. Esto permite anticipar las posibles contingencias en los sistemas e implantar medidas mitigadoras antes de que se produzcan.

4.4.4.1.2 ACCIÓN D.1.2.

Impulsar sistemas que protejan la información confidencial de seguridad en las Infraestructuras Críticas del sector

Se debe apoyar el desarrollo e implantación de sistemas que permitan establecer medidas para la protección del conocimiento tecnológico en torno a la seguridad de los operadores, de forma que se prevenga su apropiación indebida, lo cual supondría una violación de seguridad.

4.4.4.2 | Objetivo

D.2.

Sostener la mejora continua de características de seguridad en los sistemas de la infraestructura del sector energético

4.4.4.2.1 | ACCIÓN D.2.1.

Aportar incentivos para la innovación en seguridad mediante la protección de derechos de propiedad intelectual

La innovación en seguridad debe ser estimulada de parte de los departamentos o Ministerios de Energía. Para incentivar a agentes expertos se recomienda el desarrollo y protección de derechos de propiedad intelectual como patentes y copyrights.

4.4.4.2.2 | ACCIÓN D.2.2.

Respaldar la adopción de estrategias de benchmarking de ciberseguridad

Los Departamentos o Ministerios de Energía deben promover la utilización de metodologías comunes que permitan comparar el estado de la seguridad entre diferentes agentes, así como realizar ejercicios periódicamente para determinar el nivel de protección y seguridad de un operador con respecto al resto del sector.

4.4.4.2.3 | ACCIÓN D.2.3.

Reconocer la excelencia profesional en el ámbito de la ciberseguridad

Los Departamentos o Ministerios de Energía deben realizar reconocimiento, de manera oficial, a los profesionales cuyo talento y esfuerzos contribuyen al mantenimiento y mejora continua del estado de la ciberseguridad en el sector. De esta manera se fomenta la innovación en la materia y la colaboración público-privada.

05

RECOMENDACIONES A OPERADORES DEL SUBSECTOR ELÉCTRICO

5.1 | Consideraciones Generales

Los operadores del subsector eléctrico, generalmente constituidos por entidades privadas diferenciadas, son los encargados de implementar medidas en torno a la ciberseguridad sobre los sistemas donde se genera, transmite y distribuye la energía eléctrica. Estos sistemas de gestión de energía se encontrarán directamente relacionados con sistemas de gestión de información tanto TI como TO, como se esquematiza en la siguiente topología abstracta:

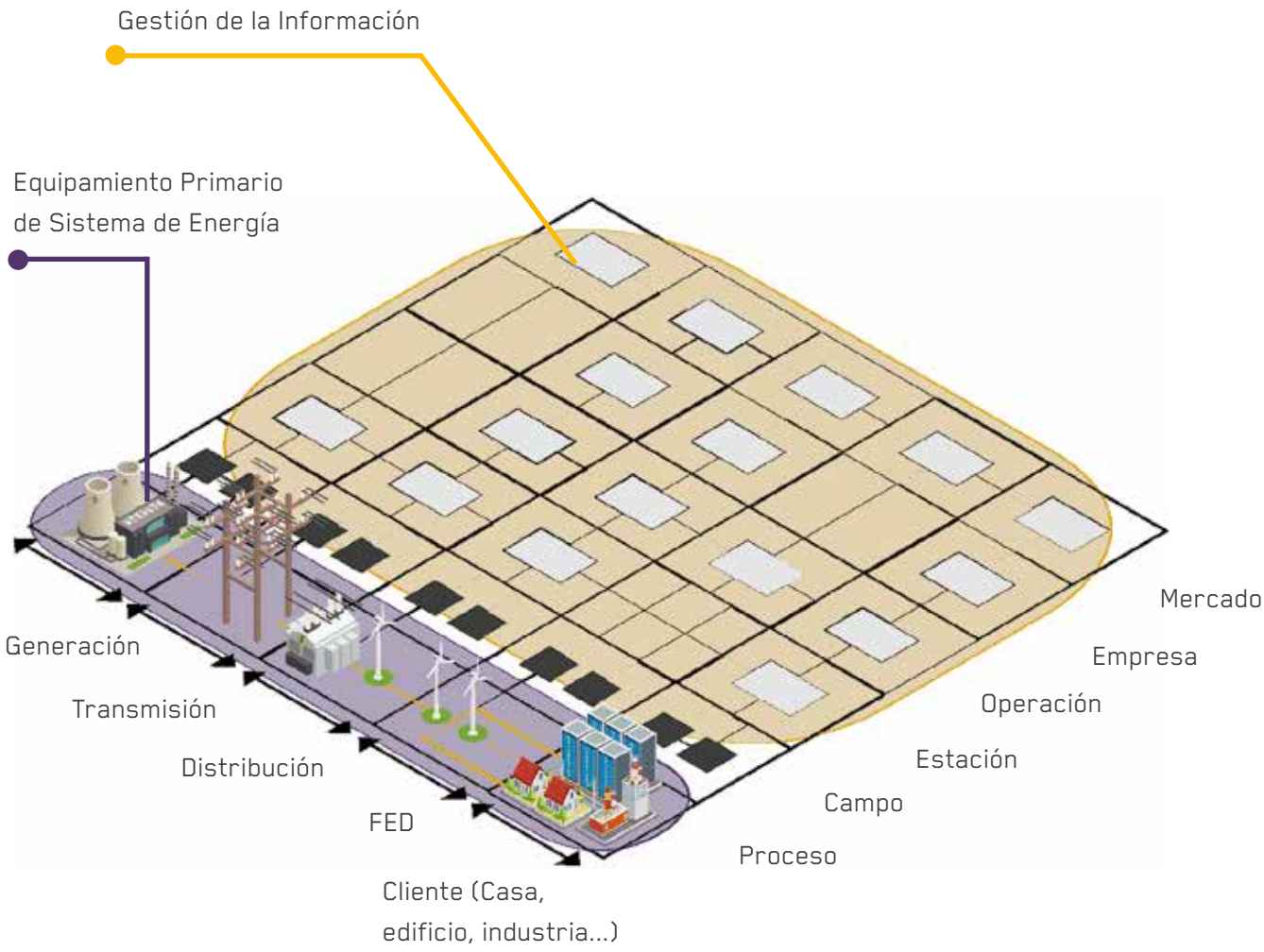


FIGURA 100. Topología de un sistema de generación de energía y la información asociada.
Fuente: Electricity Subsector C2M2 – US DoE,US DHS.

Para el citado propósito se presenta un modelo que provee una guía para ayudar a los operadores a desarrollar y mejorar sus capacidades de ciberseguridad.

El modelo se organiza en **10 dominios de ciberseguridad**, que se encuentran subdivididos en objetivos, los cuales representan consecuciones a realizar sobre el dominio.

A su vez, cada uno de los objetivos se compone de medidas organizadas en **3 niveles de madurez,** que indican el orden en que deben implementarse para alcanzar dicho objetivo.

Estas acciones deberán coordinarse con las correspondientes realizadas por el Departamento o Ministerio de Energía (apartado 4.4 del presente documento).

5.1.1 | Niveles Indicadores de la Madurez (MILs)

El marco de referencia ES-C2M2 proporciona mediante los MILs una medida de la progresión dentro de cada dominio permitiendo, a medida que se avanza en la implementación del sistema, obtener un resultado objetivo del grado de madurez alcanzado y determinar qué medidas serían recomendables para continuar mejorando en cada dominio de seguridad.

La evaluación del nivel de seguridad debe realizarse, por tanto, considerando de forma independiente en cada dominio las acciones asociadas a cada Nivel Indicador de Madurez para ese dominio específico, asignando uno de los siguientes estados:

- Totalmente implementado.
- Mayormente implementado.
- Parcialmente implementado.
- No implementado.

Deben **evaluarse** las medidas de **todos los niveles de madurez**

Deben evaluarse las medidas de todos los niveles de madurez, pues es posible que, aunque no se hayan implementado todas las acciones derivadas de un MIL determinado, sí se encuentren ya implementadas acciones de un MIL superior.

DIAGRAMA DE KIVIAT
SOBRE CUMPLIMIENTO ES-C2M2

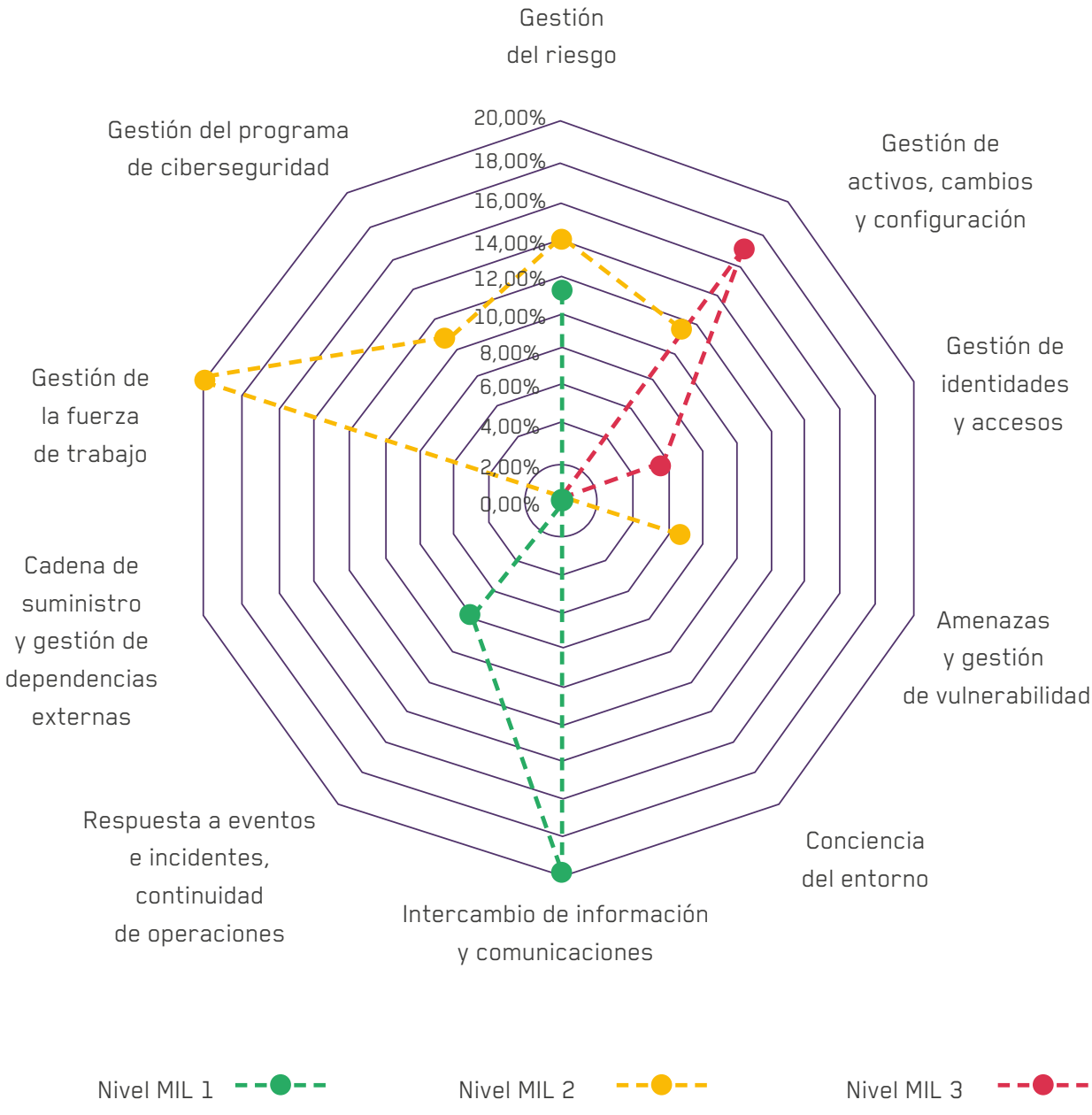


FIGURA 101. Ejemplo de Diagrama de Kiviat generado considerando los diferentes dominios de seguridad de ES-C2M2 y los Niveles Indicadores de Madurez (MIL).

5.2 Hoja de ruta y herramienta de autoevaluación para operadores del subsector eléctrico

Se describen a continuación las dimensiones tomadas del modelo ES-C2M2 [18] que se implementan en detalle en la herramienta de autoevaluación disponible en el siguiente enlace: http://bit.ly/BIDesC2M2

5.2.1 GESTIÓN DEL RIESGO

5.2.1.1 *Establecer una estrategia de gestión del riesgo de ciberseguridad*

NIVEL 1

No hay actividades para el Nivel 1.

NIVEL 2

- **a** Existe una estrategia documentada de gestión del riesgo de ciberseguridad.
- **b** La estrategia proporciona un enfoque para la priorización de riesgos, incluida la consideración del impacto.

NIVEL 3

- **c** Los criterios del riesgo de la organización (criterios objetivos que la organización utiliza para evaluar, categorizar y priorizar los riesgos operativos en función del impacto, la tolerancia al riesgo y los enfoques de respuesta al riesgo) están definidos y disponibles.
- **d** La estrategia de gestión del riesgo se actualiza periódicamente para reflejar el entorno de amenazas actual.
- **e** Se documenta una taxonomía de riesgo específica de la organización y se utiliza en actividades de gestión de riesgos.

5.2.1.2 *Gestionar el riesgo de ciberseguridad*

NIVEL 1

- **a** Se identifican riesgos de ciberseguridad.
- **b** Los riesgos identificados son mitigados, aceptados, tolerados o transferidos.

NIVEL 2

- **c** Las evaluaciones de riesgos se realizan para identificar los riesgos de acuerdo con la estrategia de gestión de riesgos.
- **d** Los riesgos identificados están documentados.
- **e** Los riesgos identificados se analizan para priorizar las actividades de respuesta de acuerdo con la estrategia de gestión de riesgos.
- **f** Los riesgos identificados se monitorean de acuerdo con la estrategia de gestión de riesgos.
- **g** El análisis de riesgos se basa en la arquitectura de red (TI y / o TO).

NIVEL 3

- **h** El programa de gestión de riesgos define y opera políticas y procedimientos de gestión de riesgos que implementan la estrategia de gestión de riesgos.
- **i** Se utiliza una arquitectura de ciberseguridad actualizada para informar el análisis de riesgos.
- **j** Se utiliza un registro de riesgos (un registro estructurado de riesgos identificados) para respaldar las actividades de gestión de riesgos.

5.2.1.3 *Actividades de gestión*

NIVEL 1

No hay actividades para el Nivel 1.

NIVEL 2

- **a** Se siguen prácticas documentadas para las actividades de gestión de riesgos.
- **b** Las partes interesadas para las actividades de gestión de riesgos se identifican y participan.
- **c** Se proporcionan recursos adecuados (personas, fondos y herramientas) para apoyar las actividades de gestión de riesgos.
- **d** Se han identificado normas y / o directrices para informar las actividades de gestión de riesgos.

NIVEL 3

- **e** Las actividades de gestión de riesgos están guiadas por políticas documentadas u otras directivas de la organización.
- **f** Las políticas de gestión de riesgos incluyen requisitos de cumplimiento para normas y / o pautas específicas.
- **g** Las actividades de gestión de riesgos se revisan periódicamente para garantizar la conformidad con la política.
- **h** La responsabilidad y la autoridad para el desempeño de las actividades de gestión de riesgos se asignan al personal.
- **i** El personal que realiza actividades de gestión de riesgos tiene las habilidades y el conocimiento necesarios para desempeñar sus responsabilidades asignadas.

5.2.2 GESTIÓN DE ACTIVOS, CAMBIOS Y CONFIGURACIÓN

5.2.2.1 *Gestionar inventario de activos*

NIVEL 1

a Existe un inventario de activos de TO y TI que son importantes para la actividad del operador.

b Existe un inventario de activos de información que son importantes para la actividad del operador (por ejemplo, puntos de ajuste SCADA, información del cliente, datos financieros).

NIVEL 2

c Los atributos del inventario incluyen información para respaldar la estrategia de ciberseguridad (por ejemplo, ubicación, activo, propietario, requisitos de seguridad aplicables, dependencias de servicio, acuerdos de nivel de servicio y conformidad de los activos con los estándares relevantes de la industria).

d Los activos inventariados se priorizan en función de su importancia para el desempeño de la actividad del operador.

NIVEL 3

e Existe un inventario para todos los activos conectados de TI y TO relacionados con la actividad del operador.

f El inventario de activos está actualizado (según lo definido por la organización).

5.2.2.2 *Administrar la configuración de activos*

NIVEL 1

a Los requisitos básicos de configuración se establecen para los activos inventariados, siendo deseable asegurar que múltiples activos se configuran de manera similar.

b Los requisitos básicos de configuración se utilizan para configurar activos en el despliegue.

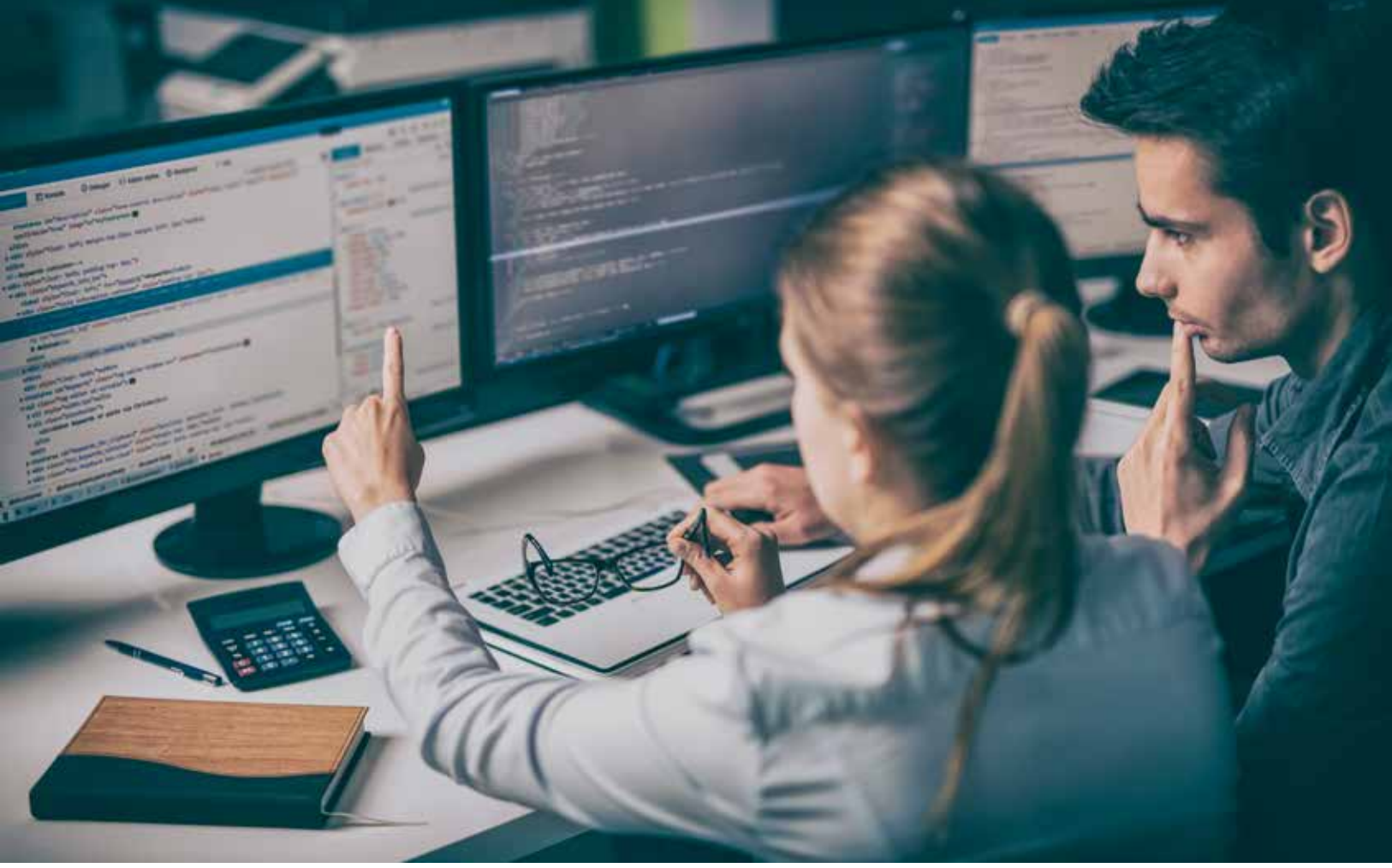
NIVEL 2

c El diseño de los requisitos básicos de configuración incluye objetivos de ciberseguridad.

NIVEL 3

d La configuración de los activos se supervisa para garantizar la coherencia con los requisitos básicos de configuración a lo largo del ciclo de vida de los activos.

e Los requisitos básicos de configuración se revisan y actualizan con una frecuencia definida por el operador.



5.2.2.3 *Gestionar cambios en los activos*

NIVEL 1

a Los cambios en los activos inventariados se evalúan antes de implementarse.

b Los cambios en los activos inventariados se registran.

NIVEL 2

c Los cambios en los activos se prueban antes de implementarse, siempre que sea posible.

d Las prácticas de gestión de cambios abordan el ciclo de vida completo de los activos (es decir, adquisición, implementación, operación, retirada).

NIVEL 3

e Los cambios en los activos se prueban para determinar el impacto en cuanto a ciberseguridad antes de implementarse.

f Los registros de cambios incluyen información sobre modificaciones que afectan a las dimensiones de seguridad de activos (disponibilidad, integridad, confidencialidad).

5.2.3 GESTIÓN DE IDENTIDADES Y ACCESOS

5.2.3.1 *Establecer y mantener identidades*

NIVEL 1

a Las identidades se provisionan para el personal y otras entidades (por ejemplo, servicios, dispositivos) que requieren acceso a los activos (teniendo en cuenta que esto no excluye las identidades compartidas).

b Se emiten credenciales para el personal y otras entidades que requieren acceso a los activos (por ejemplo, contraseñas, tarjetas inteligentes, certificados, llaves).

c Las identidades se dan de baja cuando ya no son necesarias.

NIVEL 2

d Los registros de identidad se revisan y actualizan periódicamente para garantizar su validez (es decir, para garantizar que las identidades todavía necesitan acceso).

e Las credenciales se revisan periódicamente para garantizar que estén asociadas con la persona o entidad correcta.

f Las identidades se inhabilitan dentro de los límites de tiempo definidos organizacionalmente cuando ya no se requieren.

NIVEL 3

g Los requisitos para las credenciales están alineados con los criterios de riesgo de la organización (por ejemplo, autenticación multifactor para accesos de mayor riesgo).

5.2.3.2 *Control de acceso*

NIVEL 1

- **a** Se determinan los requisitos de acceso, incluidos los de acceso remoto (los requisitos de acceso son asociados con los activos y brindan orientación sobre qué tipos de entidades pueden acceder al activo, los límites de acceso permitido y los parámetros de autenticación).
- **b** Se otorga acceso a las identidades según los requisitos.
- **c** El acceso se revoca cuando ya no es necesario

NIVEL 2

- **d** Los requisitos de acceso incorporan los principios de mínimo privilegio y segregación de funciones.
- **e** Las solicitudes de acceso son revisadas y aprobadas por el propietario del activo
- **f** Los privilegios de superusuarios, el acceso administrativo, el acceso de emergencia y las cuentas compartidas reciben más escrutinio y monitoreo.

NIVEL 3

- **g** Los privilegios de acceso se revisan y actualizan para garantizar su validez, con una frecuencia definida organizacionalmente.
- **h** El propietario del activo otorga acceso a los activos en función del riesgo para la actividad del operador.
- **i** Los intentos de acceso anómalos son monitoreados como indicadores de eventos de seguridad cibernética.

5.2.3.3 *Actividades de gestión*

NIVEL 1

No hay actividades de Nivel 1.

NIVEL 2

- **a** Se siguen prácticas documentadas para establecer y mantener identidades y controlar el acceso.
- **b** Las partes interesadas para el acceso y las actividades de gestión de identidad se identifican y participan.
- **c** Se proporcionan recursos adecuados (personas, fondos y herramientas) para apoyar el acceso e identificar actividades de gestión.
- **d** Se han identificado estándares y / o pautas para informar las actividades de acceso y gestión de identidad.

NIVEL 3

- **e** Las actividades de acceso y gestión de identidad están guiadas por políticas documentadas u otras directivas de la organización.
- **f** Las políticas de acceso y gestión de identidad incluyen requisitos de cumplimiento para estándares específicos y / o pautas.
- **g** Las actividades de acceso y gestión de identidad se revisan periódicamente para garantizar la conformidad con la política.
- **h** La responsabilidad y la autoridad para el desempeño de las actividades de acceso y gestión de identidad son asignados al personal.
- **i** La responsabilidad y la autoridad para el desempeño de las actividades de acceso y gestión de identidad son asignados al personal.

5.2.4 AMENAZAS Y GESTIÓN DE VULNERABILIDADES

5.2.4.1 *Identificar y responder a las amenazas*

NIVEL 1

- **a** Se identifican las fuentes de información para apoyar las actividades de gestión de amenazas (por ejemplo, departamentos o ministerios de energía, asociados de la industria, proveedores, informes estatales).
- **b** La información sobre amenazas de ciberseguridad se recopila e interpreta para la actividad del operador.
- **c** Se abordan las amenazas que se consideran importantes para la actividad del operador.

NIVEL 2

- **d** Se establece un perfil de amenaza para la actividad del operador que incluye la caracterización de la probabilidad, la capacidad, y objetivo de amenazas a la actividad del operador.
- **e** Las fuentes de información sobre amenazas que abordan todos los componentes del perfil de amenazas tienen prioridad y son monitoreadas.
- **f** Las amenazas identificadas se analizan y priorizan.
- **g** Las amenazas se abordan de acuerdo con la prioridad asignada.

NIVEL 3

- **h** El perfil de amenaza para la actividad del operador se valida con una frecuencia definida por la organización.
- **i** El análisis y la priorización de las amenazas se basan en los criterios de riesgo de la organización.
- **j** La información sobre amenazas se agrega al registro de riesgos.

5.2.4.2 *Reducir las vulnerabilidades de ciberseguridad*

NIVEL 1

a Se identifican las fuentes de información para respaldar el descubrimiento de vulnerabilidades de ciberseguridad (por ejemplo, asociaciones industriales, proveedores, informes federales, evaluaciones internas).

b La información de vulnerabilidad de ciberseguridad se recopila e interpreta para la actividad del operador.

c Se abordan las vulnerabilidades de ciberseguridad que se consideran importantes para la actividad del operador (por ejemplo, implementar controles de mitigación, aplicar parches de ciberseguridad).

NIVEL 2

d Las fuentes de información de vulnerabilidad de ciberseguridad que abordan todos los activos importantes para la actividad del operador son monitoreados.

e Se realizan evaluaciones de vulnerabilidad de ciberseguridad (por ejemplo, revisiones de arquitectura, pruebas de penetración, ejercicios de ciberseguridad, herramientas de identificación de vulnerabilidades).

f Las vulnerabilidades de seguridad cibernética identificadas se analizan y priorizan (por ejemplo, un sistema de puntuación de vulnerabilidades podría usarse para la apliación de parches; las pautas internas podrían usarse para priorizar otros tipos de vulnerabilidades).

g Las vulnerabilidades de ciberseguridad se abordan de acuerdo con la prioridad asignada.

h El impacto operativo en la actividad del operador se evalúa antes de implementar parches de ciberseguridad.

NIVEL 3

i Las evaluaciones de vulnerabilidad de ciberseguridad se realizan para todos los activos importantes para la actividad de la organización, a una frecuencia definida por la organización.

j Las evaluaciones de vulnerabilidad de ciberseguridad están alineadas con los criterios de riesgo de la organización.

k Las evaluaciones de vulnerabilidad de ciberseguridad son realizadas por partes independientes de operaciones de la organización.

l El análisis y la priorización de las vulnerabilidades de ciberseguridad son dirigidos por la organización.

m La información de vulnerabilidades de ciberseguridad se agrega al registro de riesgos.

n Las actividades de monitoreo de riesgos validan las respuestas a las vulnerabilidades de ciberseguridad (por ejemplo, la implementación de parches u otras actividades).

5.2.4.3 *Actividades de gestión*

NIVEL 1

Sin actividades en Nivel 1.

NIVEL 2

a Se siguen prácticas documentadas para las actividades de gestión de amenazas y vulnerabilidades.

b Las partes interesadas para las actividades de gestión de amenazas y vulnerabilidades se identifican y participan.

c Se proporcionan recursos adecuados (personas, fondos y herramientas) para soportar actividades de gestión de amenazas y vulnerabilidades.

d Se han identificado normas y / o directrices para informar actividades de gestión de amenazas y vulnerabilidades.

NIVEL 3

e Las actividades de amenazas y vulnerabilidades están guiadas por políticas documentadas u otras actividades de organización.

f Las políticas de gestión de amenazas y vulnerabilidades incluyen requisitos de cumplimiento para determinados estándares y / o pautas.

g Las actividades de gestión de amenazas y vulnerabilidades se revisan periódicamente para garantizar la conformidad con las políticas.

h Se asigna responsabilidad y autoridad para el desempeño de actividades de gestión de amenazas y vulnerabilidades al personal.

i El personal que realiza actividades de gestión de amenazas y vulnerabilidades tiene las habilidades y el conocimiento necesarios para realizar sus responsabilidades asignadas.

5.2.5 CONCIENCIA DEL ENTORNO

5.2.5.1 *Registrar eventos*

NIVEL 1

a El registro de eventos se realiza para activos importantes para la actividad del operador cuando sea posible.

NIVEL 2

b Los requisitos de registro de eventos se han definido para todos los activos importantes para la actividad del operador (por ejemplo, el alcance de actividad y cobertura de activos, requisitos de ciberseguridad [confidencialidad, integridad, disponibilidad]).

c Los datos de registro de eventos se agregan dentro de la actividad del operador.

NIVEL 3

d Los requisitos de registro de eventos se basan en el riesgo para la actividad del operador.

e Los datos de registro de eventos admiten otros procesos comerciales y de seguridad (por ejemplo, respuesta a incidentes, gestión de activos).

5.2.5.2 *Realizar monitoreo*

NIVEL 1

a Se realizan actividades de monitoreo de ciberseguridad (por ejemplo, revisiones periódicas de datos de registro).

b Los entornos operativos se controlan para detectar comportamientos anómalos que pueden indicar un evento de ciberseguridad.

NIVEL 2

c Los requisitos de monitoreo y análisis se han definido para la actividad del operador y abordan la revisión oportuna de datos de eventos.

d Las alarmas y alertas están configuradas para ayudar en la identificación de eventos de ciberseguridad.

e Se han definido indicadores de actividad anómala y se monitorean a lo largo de la operación.

f Las actividades de monitoreo están alineadas con el perfil de amenaza de la actividad del operador.

NIVEL 3

g Los requisitos de monitoreo se basan en el riesgo para la actividad del operador.

h El monitoreo está integrado con otros procesos comerciales y de seguridad (por ejemplo, respuesta a incidentes, gestión de activos).

i El monitoreo continuo se realiza en todo el entorno operativo para identificar actividades anómalas.

j El contenido del registro de riesgos se utiliza para identificar indicadores de actividad anómala.

k Las alarmas y alertas se configuran de acuerdo con indicadores de actividad anómala.

5.2.5.3 *Establecer y mantener una imagen operativa común*

NIVEL 1

No hay actividades de Nivel 1.

NIVEL 2

a Se establecen y mantienen métodos para comunicar el estado actual de ciberseguridad para la actividad del operador.

b Los datos de monitoreo se agregan para proporcionar una comprensión del estado operativo de la actividad del operador (es decir, una imagen operativa común puede o no incluir visualización o presentarse gráficamente).

c La información de toda la organización está disponible para mejorar la imagen operativa común.

NIVEL 3

d Los datos de monitoreo se agregan para proporcionar una comprensión casi en tiempo real del estado de ciberseguridad.

e Se recopila información de fuera de la organización para mejorar la imagen operativa común.

f Los estados de operación predefinidos se definen e invocan (proceso manual o automatizado) en función de la imagen operativa común.

5.2.5.4 *Actividades de gestión*

NIVEL 1

No hay actividades de Nivel 1.

NIVEL 2

a. Se siguen prácticas documentadas para las actividades de registro y monitoreo de la imagen operativa común.

b. Las partes interesadas para las actividades de registro y monitoreo de la imagen operativa común están identificadas e involucradas.

c. Se proporcionan recursos adecuados (personas, fondos y herramientas) para apoyar las actividades de registro y monitoreo de la imagen operativa común.

d. Se han identificado estándares y / o pautas para informar las actividades de registro y monitoreo de la imagen operativa común.

NIVEL 3

e. Las actividades de registro y monitoreo de la imagen operativa común están guiadas por políticas documentadas u otras directivas de la organización.

f. Las políticas de registro, monitoreo de la imagen operativa común incluyen requisitos de cumplimiento para estándares específicos y / o pautas.

g. Las actividades de registro, monitoreo de la imagen operativa común se revisan periódicamente para garantizar el cumplimiento de la política.

h. La responsabilidad y autoridad para el desempeño de las actividades de registro y monitoreo de la imagen operativa común son asignados al personal.

i. El personal que realiza actividades de registro y monitoreo de la imagen operativa común tiene las habilidades y el conocimiento necesarios para realizar sus responsabilidades asignadas.

5.2.6 INTERCAMBIO DE INFORMACIÓN Y COMUNICACIONES

5.2.6.1 *Compartir información de ciberseguridad*

NIVEL 1

a La información se recopila y se proporciona a individuos u organizaciones seleccionados.

b La responsabilidad de las obligaciones de informes de seguridad cibernética se asigna al personal.

NIVEL 2

c Las partes interesadas que comparten información se identifican en función de su relevancia para la operación continua de la actividad del operador (p. ej., servicios públicos conectados, proveedores, organizaciones sectoriales, reguladores, entidades internas).

d La información se recopila y se proporciona a las partes interesadas identificadas que comparten información.

e Se identifican fuentes técnicas que se pueden consultar sobre cuestiones de ciberseguridad.

f Se establecen y mantienen disposiciones para permitir el intercambio seguro de información confidencial o clasificada.

g Las prácticas de intercambio de información abordan tanto las operaciones estándar como las operaciones de emergencia.

NIVEL 3

h Las partes interesadas que comparten información se identifican en función del interés compartido y el riesgo para infraestructura.

i La organización participa con centros de análisis e intercambio de información.

j Los requisitos de intercambio de información se han definido y se abordan oportunamente difusión de información sobre ciberseguridad.

k Existen procedimientos para analizar y desconfiar la información recibida.

l Se ha establecido una red de relaciones de confianza internas y externas (formales y / o informales) para examinar y validar información sobre eventos cibernéticos.

5.2.6.2 *Actividades de gestión*

NIVEL 1

No hay actividades de Nivel 1.

NIVEL 2

a. Se siguen prácticas documentadas para actividades de intercambio de información.

b. Las partes interesadas para las actividades de intercambio de información se identifican y participan.

c. Se proporcionan recursos adecuados (personas, fondos y herramientas) para apoyar las actividades de intercambio de información.

d. Se han identificado normas y / o directrices para informar las actividades de intercambio de información.

NIVEL 3

e. Las actividades de intercambio de información están guiadas por políticas documentadas u otras directivas de la organización.

f. Las políticas de intercambio de información incluyen requisitos de cumplimiento para normas y / o pautas específicas.

g. Las actividades de intercambio de información se revisan periódicamente para garantizar el cumplimiento de la política.

h. La responsabilidad y la autoridad para la realización de actividades de intercambio de información se asignan al personal.

i. El personal que realiza actividades de intercambio de información tiene las habilidades y el conocimiento necesarios para realizar sus responsabilidades asignadas.

j. Las políticas de intercambio de información abordan la información protegida y el uso ético y el intercambio de información, incluida información confidencial y clasificada según corresponda.

5.2.7 RESPUESTA A EVENTOS E INCIDENTES, CONTINUIDAD DE OPERACIONES

5.2.7.1 *Detectar eventos de ciberseguridad*

NIVEL 1

a Hay un punto de contacto (persona o rol) a quien se le pueden informar los eventos de seguridad cibernética.

b Se informan eventos de seguridad cibernética detectados.

c Los eventos de ciberseguridad se registran y rastrean.

NIVEL 2

d Se establecen criterios para la detección de eventos de ciberseguridad (por ejemplo, qué constituye un evento, dónde buscar eventos).

e Existe un repositorio donde los eventos de ciberseguridad se registran según los criterios establecidos.

NIVEL 3

f La información del evento se correlaciona para respaldar el análisis de incidentes mediante la identificación de patrones, tendencias y otras características comunes.

g Las actividades de detección de eventos de ciberseguridad se ajustan en función del registro de información del riesgo y perfil de amenazas de la organización para ayudar a detectar amenazas conocidas y monitorear los riesgos identificados.

h La imagen operativa común para la actividad del operador se supervisa para admitir la identificación de eventos de ciberseguridad.

5.2.7.2 *Escalar eventos de ciberseguridad y declarar incidentes*

NIVEL 1

a Se establecen criterios para la escalada de eventos de ciberseguridad, incluidos criterios para la declaración de incidentes de ciberseguridad.

b Los eventos de ciberseguridad se analizan para respaldar la escalada y la declaración de incidentes de ciberseguridad.

c Los eventos e incidentes de ciberseguridad escalados se registran y rastrean.

NIVEL 2

d Se establecen criterios para escalar los eventos de ciberseguridad basado en el impacto potencial de la actividad del operador, incluyendo criterios de incidentes de ciberseguridad.

e Los criterios para la escalada de eventos de ciberseguridad, incluidos los criterios de declaración de incidentes de ciberseguridad, son actualizados a una frecuencia definida por la organización.

f Hay un repositorio donde se registran y rastrean hasta su cierre los eventos de seguridad cibernética escalados y los incidentes de seguridad cibernética.

NIVEL 3

g Los criterios para el escalado de eventos de ciberseguridad, incluidos los criterios de declaración de incidentes de ciberseguridad, son ajustado de acuerdo con la información del registro de riesgos de la organización y el perfil de amenazas.

h Los eventos de ciberseguridad intensificados y los incidentes de ciberseguridad declarados están alineados con la imagen operativa común.

i Los eventos de seguridad cibernética intensificados y los incidentes declarados están correlacionados para respaldar el descubrimiento de patrones, tendencias y otras características comunes.

5.2.7.3 *Intensificar la respuesta a incidentes eventos de seguridad cibernética*

NIVEL 1

a El personal de respuesta a incidentes y eventos de ciberseguridad se identifica y se asignan roles.

b Las respuestas a incidentes e incidentes de seguridad cibernética intensificados se implementan para limitar el impacto y restaurar el funcionamiento normal.

c Se realiza un informe de incidentes e incidentes de seguridad cibernética intensificados.

NIVEL 2

d La respuesta a incidentes y eventos de ciberseguridad se realiza de acuerdo con procedimientos definidos que abordan todas las fases del ciclo de vida del incidente (p. ej., triaje, manejo, comunicación, coordinación y cierre).

e Los planes de respuesta a incidentes y eventos de ciberseguridad se ejercen con una frecuencia definida por la organización.

f Los planes de respuesta a incidentes y eventos de ciberseguridad abordan los activos de TO y TI importantes para la actividad del operador.

g Se realiza capacitación para los equipos de respuesta a incidentes y eventos de seguridad cibernética.

NIVEL 3

h Se realizan análisis de causa raíz de incidentes y eventos de ciberseguridad y actividades de lecciones aprendidas, y se toman acciones correctivas.

i Las respuestas a incidentes y eventos de seguridad cibernética se coordinan con la policía y otras entidades gubernamentales según corresponda, incluido el apoyo para la recolección y preservación de evidencia.

j El personal de respuesta a incidentes y eventos de ciberseguridad participa en ejercicios conjuntos de ciberseguridad con otras organizaciones (p. ej., incidentes simulados).

k Los planes de respuesta a incidentes y eventos de ciberseguridad se revisan y actualizan con una frecuencia definida por la organización.

l Las actividades de respuesta a incidentes y eventos de ciberseguridad se coordinan con entidades externas relevantes.

m Los planes de respuesta a incidentes y eventos de ciberseguridad están alineados con los criterios de riesgo de la actividad del operador y con los perfiles de amenaza.

n Las políticas y procedimientos para reportar eventos de seguridad cibernética e información de incidentes a las autoridades designadas cumplen con las leyes, regulaciones y acuerdos contractuales aplicables.

o Los activos restaurados se configuran adecuadamente y la información de inventario se actualiza después de la ejecución de planes de respuesta.

5.2.7.4 *Plan de continuidad*

NIVEL 1

a Se identifican las actividades necesarias para mantener las operaciones mínimas de la actividad del operador.

b Se identifica la secuencia de actividades necesarias para devolver la actividad del operador al funcionamiento normal.

c Se desarrollan planes de continuidad para mantener y restaurar el funcionamiento de la actividad del operador.

NIVEL 2

d El desarrollo de planes de continuidad se alinea con los resultados del análisis de impacto.

e Se incorporan tiempo de recuperación objetivos (RTO) y puntos de recuperación objetivos (RPO) en los planes de continuidad.

f Los planes de continuidad son evaluados y probados.

NIVEL 3

g Los análisis de impacto empresarial se revisan y actualizan periódicamente.

h RTO y RPO están alineados con los criterios de riesgo de la actividad del operador.

i Los resultados de la prueba y / o activación del plan de continuidad se comparan con los objetivos de recuperación y los planes se mejoran en consecuencia.

j Los planes de continuidad se revisan y actualizan periódicamente.

k Los activos restaurados se configuran adecuadamente y la información de inventario se actualiza después de la ejecución de planes de continuidad.

5.2.7.5 *Actividades de gestión*

NIVEL 1

No hay actividades de Nivel 1.

NIVEL 2

a Se siguen prácticas documentadas para eventos de ciberseguridad y respuesta a incidentes, así como continuidad de las actividades operativas.

b Se identifican e involucran partes interesadas en eventos de ciberseguridad y respuesta a incidentes, así como la continuidad de las actividades operativas.

c Se proporcionan recursos adecuados (personas, fondos y herramientas) para apoyar eventos de seguridad cibernética y respuesta a incidentes, así como la continuidad de las actividades operativas.

d Se han identificado estándares y / o pautas para informar eventos e incidentes de seguridad cibernética, así como la continuidad de las actividades operativas.

NIVEL 3

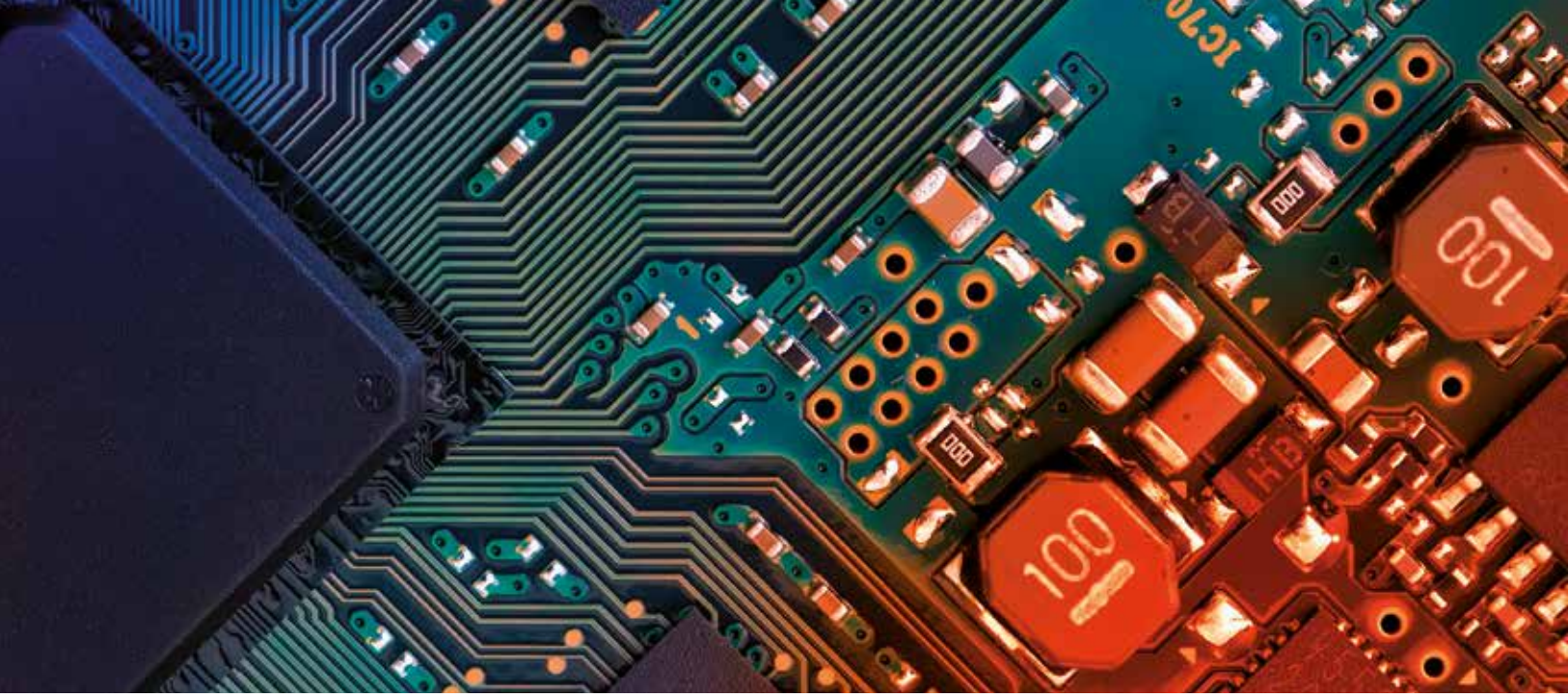
e Los eventos de ciberseguridad y la respuesta a incidentes, así como la continuidad de las actividades operativas, se guían por políticas documentadas u otras directivas organizacionales.

f La respuesta a incidentes y eventos de ciberseguridad, así como las políticas de continuidad de operaciones incluyen requisitos de cumplimiento para normas y / o pautas especificadas.

g La respuesta a incidentes y eventos de seguridad cibernética, así como la continuidad de las actividades operativas son revisados periódicamente para garantizar la conformidad con la política.

h Se asignan al personal la responsabilidad y autoridad para la realización de eventos de ciberseguridad y respuesta a incidentes, así como la continuidad de actividades operativas.

i El personal que realiza eventos de seguridad cibernética y respuesta a incidentes, así como la continuidad de las actividades operativas tiene las habilidades y el conocimiento necesarios para desempeñar sus responsabilidades asignadas.



5.2.8 CADENA DE SUMINISTRO Y GESTIÓN DE DEPENDENCIAS EXTERNAS

5.2.8.1 *Identificar dependencias*

NIVEL 1

a Se identifican dependencias importantes de proveedores de TI y TO (es decir, partes externas de las que la organización, incluidos los socios operativos).

b Se identifican dependencias importantes del cliente (es decir, partes externas que dependen de la organización, incluidos los socios operativos).

NIVEL 2

c Las dependencias de los proveedores se identifican según los criterios establecidos.

d Las dependencias del cliente se identifican según los criterios establecidos.

e Se identifican dependencias de una única fuente posible o esencial.

f Se asigna una prioridad a las dependencias.

NIVEL 3

g La identificación y la priorización de dependencias se basan en los criterios de riesgo de la organización.

5.2.8.2 *Gestionar el riesgo de dependencia*

NIVEL 1

a Se identifican y abordan riesgos significativos de ciberseguridad debido a proveedores y otras dependencias.

b Los requisitos de ciberseguridad se consideran al establecer relaciones con proveedores y otros terceros.

NIVEL 2

c Los riesgos cibernéticos de cadena de suministro identificados se registran en el registro de riesgos.

d Los contratos y acuerdos con terceros incorporan el intercambio de información sobre amenazas de ciberseguridad.

e Los requisitos de ciberseguridad se establecen para los proveedores de acuerdo con una práctica definida, incluyendo requisitos para prácticas seguras de desarrollo de software cuando sea apropiado.

f Los acuerdos con proveedores y otras entidades externas incluyen requisitos de ciberseguridad.

g La evaluación y selección de proveedores y otras entidades externas incluye la consideración de su capacidad para cumplir con los requisitos de ciberseguridad.

h Los acuerdos con los proveedores requieren la notificación de incidentes de ciberseguridad relacionados con la entrega del producto o servicio.

i Los proveedores y otras entidades externas son revisados periódicamente por su capacidad para cumplir continuamente con los requisitos de ciberseguridad.

NIVEL 3

j Los riesgos de ciberseguridad debidos a dependencias externas se gestionan de acuerdo con los criterios de riesgo de la organización.

k Los requisitos de ciberseguridad se establecen para las dependencias de los proveedores en función de los criterios de riesgo de la organización.

l Los acuerdos con los proveedores requieren la notificación de defectos del producto que inducen vulnerabilidades en el ciclo de vida previsto de los productos entregados.

m Las pruebas de aceptación de los activos adquiridos incluyen pruebas de requisitos de seguridad cibernética.

n Las fuentes de información se monitorean para identificar y evitar amenazas de la cadena de suministro (por ejemplo, elementos falsificados, software y servicios).

5.2.8.3 *Actividades de gestión*

NIVEL 1

No hay actividades de Nivel 1.

NIVEL 2

- **a** Se siguen prácticas documentadas para gestionar el riesgo de dependencia.
- **b** Las partes interesadas para gestionar el riesgo de dependencia se identifican y participan.
- **c** Se proporcionan recursos adecuados (personas, fondos y herramientas) para respaldar las actividades de gestión del riesgo de dependencia.
- **d** Se han identificado estándares y / o pautas para informar la gestión del riesgo de dependencia.

NIVEL 3

- **e** Las actividades de gestión del riesgo de dependencia están guiadas por políticas documentadas u otras directivas organizaciones.
- **f** Las políticas de gestión del riesgo de dependencia incluyen requisitos de cumplimiento para estándares específicos y / o pautas.
- **g** Las actividades de gestión del riesgo de dependencia se revisan periódicamente para garantizar la conformidad con la política.
- **h** La responsabilidad y la autoridad para el desempeño de la gestión del riesgo de dependencia se asignan al personal.
- **i** El personal que realiza la gestión del riesgo de dependencia tiene las habilidades y el conocimiento necesarios para cumplir con sus responsabilidades asignadas.

5.2.9 GESTIÓN DE LA FUERZA DE TRABAJO

5.2.9.1 *Asignar responsabilidades de ciberseguridad*

NIVEL 1

- **a** Se identifican las responsabilidades de ciberseguridad.
- **b** Las responsabilidades de ciberseguridad se asignan a personas específicas.

NIVEL 2

- **c** Las responsabilidades de ciberseguridad se asignan a roles específicos, incluidos los proveedores de servicios externos.
- **d** Las responsabilidades de ciberseguridad están documentadas (por ejemplo, en las descripciones de los puestos).

NIVEL 3

- **e** Las responsabilidades de ciberseguridad y los requisitos laborales se revisan y actualizan según corresponda.
- **f** Las responsabilidades de ciberseguridad están incluidas en los criterios de evaluación del desempeño laboral.
- **g** Las responsabilidades de ciberseguridad asignadas se gestionan para garantizar la adecuación y la redundancia de su alcance.

5.2.9.2 *Controlar el ciclo de vida laboral*

NIVEL 1

- **a** La verificación del personal (p. ej., verificación de antecedentes, pruebas de drogas) se encomienda a posiciones que tienen acceso a los activos necesarios esenciales en la actividad del operador.
- **b** Los procedimientos de terminación de personal abordan la ciberseguridad.

NIVEL 2

- **c** La verificación de personal se realiza con una frecuencia definida por la organización para los puestos que tienen acceso a los activos necesarios para la actividad del operador.
- **d** Los procedimientos de transferencia de personal abordan la ciberseguridad.

NIVEL 3

- **e** Las designaciones de riesgo se asignan a todas las posiciones que tienen acceso a los activos necesarios para la actividad del operador.
- **f** La verificación se realiza para todos los puestos (incluidos los empleados, proveedores y contratistas) a un nivel acorde al riesgo de su posición desempeñada.
- **g** La planificación de la sucesión se realiza para el personal en función de la designación del riesgo.
- **h** Se implementa un proceso formal de responsabilidad que incluye acciones disciplinarias para el personal que no cumple con las políticas y procedimientos de seguridad establecidos.

5.2.9.3 *Desarrollar una fuerza laboral de ciberseguridad*

NIVEL 1

a La capacitación en ciberseguridad se pone a disposición del personal con responsabilidades asignadas de ciberseguridad.

NIVEL 2

b Se identifican ausencias de conocimiento y habilidades de ciberseguridad.

c Las brechas identificadas se abordan a través del reclutamiento y / o capacitación.

d La capacitación en ciberseguridad se proporciona como un requisito previo para otorgar acceso a los activos que respaldan las actividades del operador (por ejemplo, capacitación de personal nuevo, capacitación de transferencia de personal).

NIVEL 3

e Se establecen y mantienen objetivos de gestión de la fuerza laboral de ciberseguridad que respaldan las necesidades operativas actuales y futuras.

f El reclutamiento y la retención están alineados para apoyar los objetivos de gestión de la fuerza laboral de ciberseguridad.

g Los programas de capacitación están alineados para apoyar los objetivos de gestión de la fuerza laboral de ciberseguridad.

h La efectividad de los programas de capacitación se evalúa con una frecuencia definida por la organización y las mejoras se realizan según corresponda.

i Los programas de capacitación incluyen educación continua y oportunidades de desarrollo profesional para personal con responsabilidades significativas de ciberseguridad.

5.2.9.4 *Aumentar la conciencia de ciberseguridad*

NIVEL 1

a Se realizan actividades de sensibilización sobre ciberseguridad.

NIVEL 2

b Se establecen y mantienen objetivos para las actividades de sensibilización sobre ciberseguridad.

c El contenido de concienciación de ciberseguridad se basa en el perfil de amenazas de la organización.

NIVEL 3

d Las actividades de concientización sobre ciberseguridad están alineadas con los estados de operación predefinidos.

e La eficacia de las actividades de sensibilización sobre ciberseguridad se evalúa en una frecuencia definida por la organización y las mejoras son realizadas según corresponda.

5.2.9.5 *Actividades de gestión*

NIVEL 1

No hay actividades de Nivel 1.

NIVEL 2

a Se siguen prácticas documentadas para las actividades de gestión de la fuerza laboral de ciberseguridad.

b Las partes interesadas para las actividades de gestión de la fuerza laboral de ciberseguridad se identifican y participan.

c Se proporcionan recursos adecuados (personas, fondos y herramientas) para apoyar las actividades de gestión de la fuerza laboral de ciberseguridad.

d Se han identificado estándares y / o pautas que se alinean con las actividades gestión de la fuerza laboral de seguridad cibernética.

NIVEL 3

e Las actividades de gestión de la fuerza laboral de ciberseguridad se guían por políticas documentadas u otras directivas organizacionales.

f Las políticas de gestión de la fuerza laboral de ciberseguridad incluyen requisitos de cumplimiento para determinados estándares y / o pautas.

g Las actividades de gestión de la fuerza laboral de ciberseguridad se revisan periódicamente para garantizar la conformidad con política.

h La responsabilidad y autoridad para el desempeño de las actividades de gestión de la fuerza laboral de ciberseguridad son asignadas al personal.

i El personal que realiza actividades de gestión de la fuerza laboral de ciberseguridad tiene las habilidades y el conocimiento necesarios para realizar sus responsabilidades asignadas.

5.2.10 GESTIÓN DEL PROGRAMA DE CIBERSEGURIDAD

5.2.10.1 *Establecer la estrategia del programa de ciberseguridad*

NIVEL 1

a La organización tiene una estrategia de programa de ciberseguridad.

NIVEL 2

b La estrategia del programa de ciberseguridad define objetivos para las actividades de ciberseguridad de la organización.

c La estrategia y las prioridades del programa de ciberseguridad están documentadas y alineadas con los objetivos estratégicos de la organización y el riesgo soportado como infraestructura crítica.

d La estrategia del programa de ciberseguridad define el enfoque de la organización para proporcionar supervisión del programa y gobierno para actividades de ciberseguridad.

e La estrategia del programa de ciberseguridad define la estructura y organización del programa de ciberseguridad.

f La estrategia del programa de ciberseguridad es aprobada por la alta dirección.

NIVEL 3

g La estrategia del programa de ciberseguridad se actualiza para reflejar los cambios comerciales, los cambios en el funcionamiento entorno y cambios en el perfil de amenaza.

5.2.10.2 *Patrocinar el programa de ciberseguridad*

NIVEL 1

- **a** Se proporcionan recursos (personas, herramientas y financiación) para apoyar el programa de seguridad cibernética.
- **b** La alta gerencia patrocina el programa de seguridad cibernética.
- **g** Se patrocina el desarrollo y mantenimiento de políticas de ciberseguridad.
- **h** La responsabilidad del programa de ciberseguridad se asigna a un rol con la autoridad requerida.

NIVEL 2

- **c** El programa de seguridad cibernética se establece de acuerdo con la estrategia de éste.
- **d** Se proporcionan fondos y otros recursos adecuados (es decir, personas y herramientas) para establecer y operar un programa de ciberseguridad alineado con su estrategia.
- **e** El patrocinio de la alta gerencia para el programa de seguridad cibernética es visible y activo (por ejemplo, la importancia y el valor de las actividades de ciberseguridad se comunican regularmente por la alta dirección).
- **f** Si la organización desarrolla o adquiere software, las prácticas seguras de desarrollo de software se fomentan como un elemento del programa de ciberseguridad.

NIVEL 3

- **i** El rendimiento del programa de ciberseguridad se controla para garantizar que se alinee con la estrategia de éste.
- **j** El programa de ciberseguridad es revisado de forma independiente (es decir, por revisores que no están en el programa) para verificar el logro de sus objetivos.
- **k** El programa de seguridad cibernética aborda y permite el logro del cumplimiento normativo pertinente.
- **l** El programa de ciberseguridad monitorea y / o participa en estándares o iniciativas seleccionados de ciberseguridad de la industria.

5.2.10.3 *Establecer y mantener la arquitectura de ciberseguridad*

NIVEL 1

a Se implementa una estrategia para aislar arquitectónicamente los sistemas de TI de la organización de los sistemas TO.

c La segmentación de arquitectura y el aislamiento se mantienen de acuerdo con un plan documentado.

NIVEL 2

b Existe una arquitectura de ciberseguridad para permitir la segmentación, el aislamiento y otros requisitos que apoyan la estrategia de ciberseguridad.

NIVEL 3

d La arquitectura de ciberseguridad se actualiza a una frecuencia definida por la organización para mantenerla actualizada.

5.2.10.4 *Realizar un desarrollo de software seguro*

NIVEL 1

No hay actividades de Nivel 1.

NIVEL 2

a El software que se implementará en activos que son importantes para la actividad de la organización se desarrolla utilizando prácticas seguras de desarrollo de software.

NIVEL 3

b Las políticas requieren que el software que se implemente en activos que son importantes para la actividad de la organización se desarrollará utilizando prácticas seguras de desarrollo de software.

5.2.10.5 *Actividades de gestión*

NIVEL 1

No hay actividades de Nivel 1.

NIVEL 2

a Se siguen prácticas documentadas para las actividades de gestión del programa de ciberseguridad.

b Las partes interesadas para las actividades de gestión del programa de ciberseguridad se identifican y participan.

c Se han identificado normas y / o directrices con las que se alinean las actividades de gestión del programa de ciberseguridad.

NIVEL 3

d Las actividades de gestión del programa de ciberseguridad se guían por políticas documentadas u otras directivas organizacionales.

e Las actividades de gestión del programa de ciberseguridad se revisan periódicamente para garantizar la conformidad con las políticas.

f El personal que realiza actividades de gestión del programa de ciberseguridad tiene las habilidades y el conocimiento necesarios para realizar sus responsabilidades asignadas.

06 CONCLUSIONES

El presente informe elaborado a solicitud del **Banco Interamericano de Desarrollo** elaborado por las consultoras **GOVERTIS Advisory Services y SCADASUDO** analiza el nivel actual de madurez de la ciberseguridad en la Industria de la energía eléctrica en América Latina y el Caribe (ALC).

Para determinar el estado del arte se ha procedido a la realización de entrevistas con actores del sector energético, incluyendo participantes en la generación, transmisión, distribución y operación del sistema, con actividad en una o varias de las áreas anteriores (2.3.1).

Como resultado de esas entrevistas, se han determinado las siguientes consideraciones, agrupadas en función de su naturaleza, haciendo referencia a los apartados del informe que permiten profundizar en las conclusiones aquí destacadas.

6.1 | Consideraciones generales y factores de riesgo

Desde la perspectiva regional, las encuestas sectoriales previas evidencian porcentajes muy elevados en la creencia de una probabilidad (de hasta un 68%) de ser víctimas de ciberataques sobre la infraestructura tecnológica de operación (3.1), resultando las tipologías de incidentes que despiertan una mayor inquietud las siguientes (3.2):

- Ataques dirigidos y APT
- Malware convencional y nuevos virus
- Ataques de Ramsomware
- Filtración de datos y espionaje
- Sabotaje u otro daño físico intencional causado por actores externos

Las inquietudes de los entrevistados contrastan con la evidencia de las tipologías de ataques que se encuentran como causa principal de los ciberincidentes detectados (3.2):

- Malware convencional y nuevos virus.
- Ataques de ramsomware.
- Errores de los empleados y acciones no intencionales.
- Amenazas desde terceras partes como la cadena de suministro o proveedores.
- Fallas en el hardware.

El **presente estudio** permite avanzar en el **conocimiento** del **estado de la ciberseguridad,** pero también emitir una serie de **recomendaciones para operadores de infraestructuras** críticas del **sector eléctrico** y para **formuladores de políticas,** incluyendo las figuras de legisladores y reguladores **nacionales y regionales**.

A modo de resumen, destacamos las siguientes conclusiones de análisis y recomendaciones, con referencia a los apartados que fundamentan la conclusión, segmentándolas para operadores de infraestructuras y formuladores de políticas.

6.2 | Operadores de infraestructuras

6.2.1 | Consideraciones Técnicas

- Existe una tendencia sectorial hacia la adquisición de tecnología de los fabricantes o de distribuidores mayoristas que prestan servicios especializados que permiten dotar de un enfoque homogéneo a las propuestas que requieren de la adquisición a múltiples fabricantes (3.4.1).

- Los empleados debidamente formados constituyen generalmente el soporte de primer y segundo nivel (3.4.2).

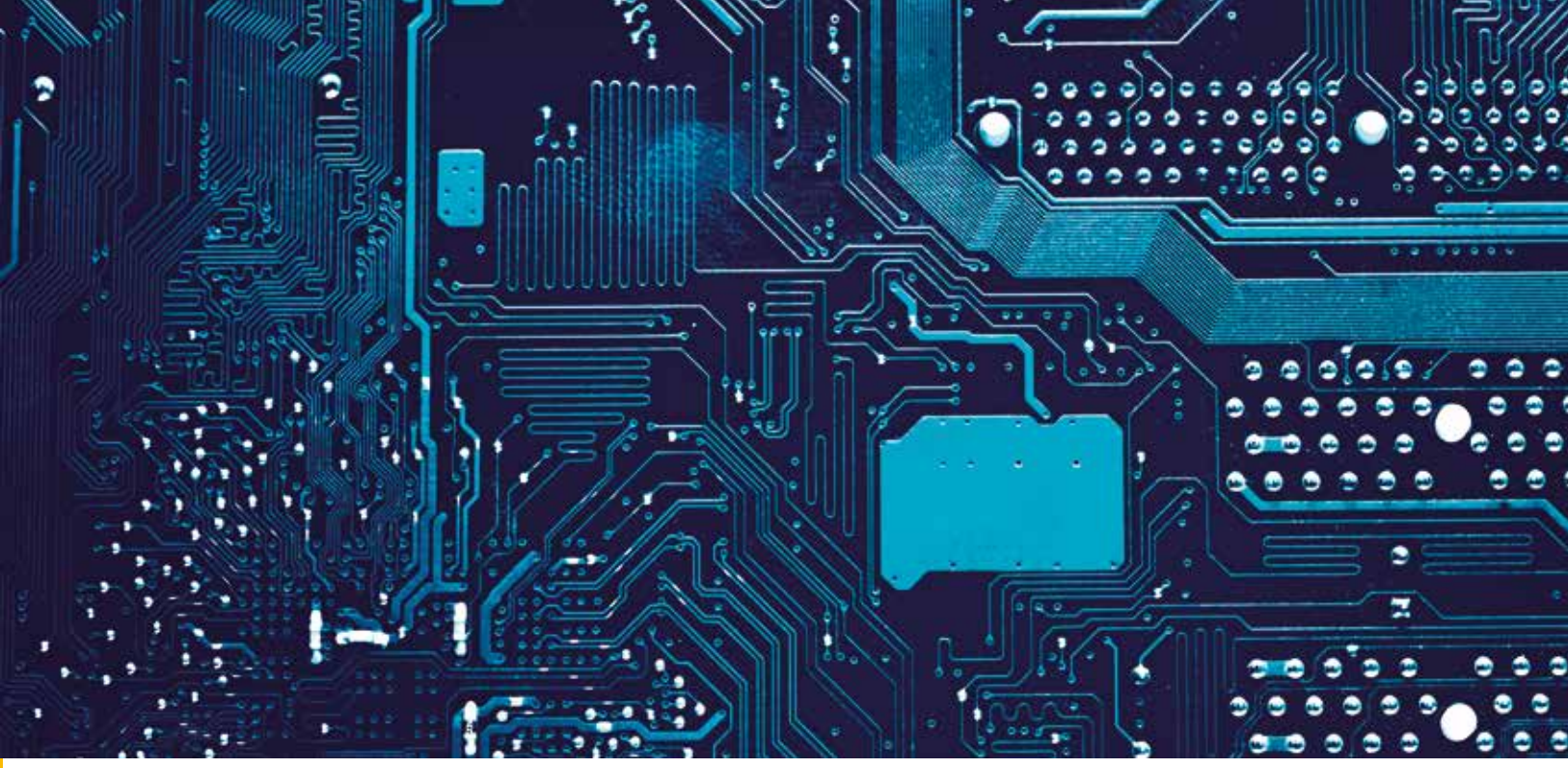
- El soporte de tercer y cuarto nivel es prestado por fabricantes o distribuidores mayoristas, especialmente en el caso de requerir considerar las consecuencias sobre otros dispositivos en instalaciones multifabricante (3.4.3).

- La mayoría de los actores sectoriales han desplegado una única red en la organización incluyendo separación de la red operacional y corporativa, o bien redes diferentes para cada una de las instalaciones con separación entre subredes en cada instalación (3.4.4).

- Aproximadamente la mitad de las redes de operación están conectadas a Internet a través de sus redes corporativas (2.4.4), llegando este porcentaje a prácticamente el 100% en los actores del segmento de Transmisión (3.4.4).

- Existe un entorno heterogéneo en cuanto a la gestión de backups y de la seguridad a través de VLANs especializadas (3.4.4).

- La conexión no controlada de equipos a redes de operación es factible en un gran número de actores, bien sea por no contar con un NAC (65% de los encuestados) o por la ausencia de otros controles alternativos o compensatorios (3.4.5).



- El acceso remoto a las redes de operación a través de Internet es una práctica generalizada en el sector, derivada de los procesos de mantenimiento y control actualmente desplegados, tanto internos como con proveedores. Consecuentemente, no siempre es requerido el acceso a través de la red corporativa, no teniendo visibilidad sobre los mecanismos de autenticación y autorización de los proveedores (3.4.5).

- La administración remota es una funcionalidad estándar de los dispositivos (3.4.5).

- Existe todavía un importante número de dispositivos cuya función de administración remota de dispositivos se realiza utilizando protocolos obsoletos o que no disponen de medidas de seguridad robustas, como SNMP versiones 1 y 2 (3.4.5).

- De igual modo, cuando las redes de operación disponen de redes inalámbricas Wi-Fi no se está utilizando en un gran número de ocasiones el protocolo WPA3, sino versiones previas o protocolos considerados no seguros (3.4.5).

- Se ha detectado también la no utilización de firewalls especializados en protocolos industriales para la protección de redes de operación, no siendo efectivos contra amenazas específicas (3.4.5).

- Funciones generalmente propias del firewall en entornos securizados, como el enrutamiento hacia todas las VLANs o la limitación del uso en las redes únicamente de los protocolos autorizados, no siempre son forzadas en los entornos que disponen de dispositivos firewall desplegados (3.4.5).

- En gran parte de los entornos no se han definido políticas específicas de bastionado de firewalls, siendo utilizadas únicamente como referencia las recomendaciones genéricas de los fabricantes (3.4.5).

6.2.2 | Control de Acceso, Autorización y Bastionado

- El acceso a las redes se produce automáticamente en función de políticas corporativas del directorio para un número significativo de actores, sin tener procedimientos de aprobación individual a zonas de seguridad sensibles (3.4.5).

- La utilización de contraseñas comunes para diferentes dispositivos de red es una práctica frecuente, constituyendo puntos únicos de fallo su difusión no autorizada o su no actualización periódica (3.4.5).

- En cuanto a servidores de control, el uso de contraseñas compartidas e, incluso, de contraseñas de fabricantes, es una práctica común (3.4.5).

- Muy pocos actores han adoptado medidas de bastionado de los PLCs, siendo 25 los entrevistados que manifiestan que no adoptan ninguna medida de bastionado sobre los mismos, como el bloqueo físico de puertos de conexión no utilizados o la desactivación de aplicaciones y servicios innecesarios (3.4.5, 3.4.7.4).

- En contraste, el bastionado de las estaciones de ingeniería y los servidores de control se encuentra más maduro por su semejanza a los entornos TI, siendo requerido reforzar las políticas relacionadas y la actualización del firmware (3.4.5, 3.4.7.4).

- Únicamente un 7% de los entrevistados han adoptado acciones orientadas a la protección ante medios extraíbles o fugas de datos, incluyendo la adopción de tecnologías DLP o similares especializadas o habilitadas por sus dispositivos firewall (3.4.5).

- El proceso de autorización de acceso a los sistemas para nuevos usuarios externos requiere procesos de aprobación que implican el nombramiento de supervisores y, en un gran número de actores, la implicación de los administradores de red e, incluso, de Recursos Humanos (3.4.7.3).

- Únicamente un 8% de los entrevistados dispone de políticas de conexión remota definidas, resultando un proceso inmaduro sujeto a la discreción de los administradores o de los autorizadores la concesión del acceso remoto y, con ello, la creación de un conducto con acceso a través de una red pública a una zona de seguridad (3.4.7.3).

6.2.3 | Compromiso de Dirección, Política, Roles y Responsabilidades

- Un 16% de los actores manifiesta que cuentan con el apoyo de dirección pero no cuentan con un presupuesto dedicado para la ciberseguridad industrial, evidenciando una falta de compromiso y concienciación sobre los riesgos operacionales a los que expone los procesos de la compañía (3.4.7.1).

- La difusión y actualización de la Política de Seguridad de la compañía debe mejorarse para fomentar la concienciación y formación de los empleados existentes y las nuevas incorporaciones, pudiendo mejorarse en su formulación actual con un mayor alineamiento con mejores prácticas como NERC, NIST o ISO 27001 (3.4.7.1).

- La ciber-resiliencia o capacidad de resistencia ante ataques cibernéticos es una capacidad que requiere de un mayor foco de la organización, requiriendo de auditorías y revisiones periódicas, así como de un nuevo enfoque en ingeniería ciber-resiliente (3.4.7.1).

- La frecuencia de las auditorías y controles periódicos es insuficiente para entornos tan críticos con consecuencias directas tanto para la organización como para la sociedad en su conjunto (3.4.7.1).

- La función de Responsable de Seguridad o CISO dedicado en las compañías todavía no se encuentra suficientemente generalizado, siendo requerido para su ejercicio que cuente con la experiencia y certificaciones necesarias (3.4.7.1).

- En instalaciones distribuidas, la seguridad requiere la designación de responsables regionales que cuenten con la cualificación y certificaciones oportunas (3.4.7.1).

6.2.4 | Monitorización de la Seguridad

- Un aspecto crítico para el buen gobierno de la seguridad es la medición. Para ello, el registro de los eventos significativos y el monitoreo de esas ocurrencias resulta la base fundamental para conocer qué está ocurriendo en las redes. Hasta 11 actores manifiestan un monitoreo escaso o nulo de sus redes. Entre aquellos que las monitorean, un 14% utilizan tecnologías no especializadas en entornos industriales, careciendo, por tanto, de visibilidad sobre las amenazas específicas de esos entornos (3.4.7.2).

- Una vez se elevan alertas a partir de los eventos detectados, más de un 50% de las compañías no puede hacer una correcta gestión del incidente por carecer de procedimientos específicos o profesionales especializados en entornos industriales (3.4.7.2).

6.2.5 | Seguridad Física

- La seguridad física se encuentra más madura, con soluciones de CCTV y centro de control desplegadas en un gran número de actores e instalaciones y medidas maduras de vigilancia física y control de acceso físico para el personal interno y visitantes externos (3.4.7.3).

- Procede reforzar las medidas de escolta a las visitas durante toda su estancia en las zonas de seguridad más críticas (3.4.7.3).

- Uno de los mayores vectores de riesgo se identifica con la conexión directa y con escaso control por parte de los técnicos de los proveedores, de sus propios equipos y dispositivos de almacenamiento, constituyendo un conducto de entrada no controlado a la zona de seguridad y una fuente de propagación inmediata de malware (3.4.7.3).

6.2.6 | Continuidad de las operaciones

- Las copias de seguridad y la redundancia en la infraestructura, como medidas esenciales para garantizar la continuidad de las operaciones y una rápida recuperación, son medidas ampliamente utilizadas por los diferentes actores (3.4.7.5).

- Los porcentajes de cobertura de las copias de seguridad deberían ser superiores para elementos críticos de la infraestructura TO (3.4.7.5).

6.3 | Recomendaciones

6.3.1 | Recomendaciones para Formuladores de Política Pública

El cuerpo de legisladores tiene el mandato de generar un marco legal que le permita al Estado brindar un ambiente óptimo para que la sociedad prospere, por ello es uno de los actores a quienes se dirigen las siguientes conclusiones. Se destacan aquí la adopción de medidas necesarias para la creación de un marco común de seguridad, incluyendo:

- La completitud de la identificación de las infraestructuras críticas y sus operadores (4.2).
- El desarrollo de una estrategia de seguridad específica para un sector tan crítico como el energético (4.2).
- El fomento a la colaboración nacional e internacional para el conocimiento sobre el estado de la seguridad (situational awareness) y su monitorización, dado el carácter transnacional de las redes energéticas (4.2).
- La coordinación de acciones a través de equipos de respuesta a incidentes formados específicamente para escenarios materializados sobre tecnologías de operación y, en concreto, sobre activos del sector energético (4.2).
- El diseño de programas de formación, cualificación y certificación de las capacidades específicas requeridas para la identificación, prevención, detección, respuesta y recuperación ante esta tipología de ciberincidentes (4.3).
- La formalización de una hoja de ruta que cuente con la participación del sector, pero también de expertos independientes, que permita avanzar en los objetivos anteriores, considerando las inquietudes y la relevancia económica del sector, pero también el rol del formulador de políticas como responsable último del gobierno de los riesgos que puedan afectar a la sociedad en general (4.4).

6.3.2 | Recomendaciones específicas para las empresas del sector eléctrico

Se presentan las siguientes conclusiones específicas siguiendo el modelo de solución de problemas y gestión del riesgo conocido como las 5M. Estas cubren los siguientes aspectos: máquina (*machine*), método (*management*), mano de obra (*man*), medio ambiente (*medium*) y misión (*mission*). Las medidas están orientadas a considerar acciones específicas que puedan ser implementadas en cada país por parte de los actores relevantes del sector eléctrico.

MÁQUINA

- Se recomienda considerar la ciberseguridad del sector con un enfoque de cadena de suministro. Cada tipo de empresa cumple un rol y la afectación de una empresa puede propagarse al resto de la cadena y generar resultados catastróficos en la operación y afectar la calidad del servicio crítico.

- Al momento de confiar que el soporte de primero, segundo y tercer nivel se dé por personal interno, la organización debe garantizar que el personal esté constantemente capacitado y actualizado para que sea capaz de atender y resolver cualquier evento que se produzca en su entorno.

- Generar una transición entre seguridad por oscuridad a seguridad por defectos y seguridad por capas debe ser uno de los principios rectores en la operación.

- Como acciones de mitigación, es recomendable donde se requiera, la implementación de múltiples factores de autenticación para acceder local o remotamente a los dispositivos críticos de la red.

MÉTODO

- Es necesario que las empresas implementen un sistema de gestión para gobernar la seguridad de la información en su infraestructura TO.

- Este sistema de gestión debe estar basado en marcos de buenas prácticas industriales como pueden ser NERC CIP, ISA 62443, NIST CSF, o ES-C2M2.

- En relación con la ciberseguridad es recomendable que las valoraciones relacionadas con la confidencialidad y la integridad sean tratadas con la misma prioridad que la disponibilidad, para no generar vulnerabilidades que afecten seriamente la operación.

- Como parte del sistema de gestión, las empresas deben implantar la gestión del riesgo como mecanismo para la toma de decisión. Esto permite garantizar que se pase de un proceso reactivo de la seguridad a uno completamente proactivo que conduzca a la resiliencia.

- La gestión de riesgo también se debe extender a la manera como los estados deban proteger sus infraestructuras críticas ante ciberataques.

- Es importante que cada empresa defina unos indicadores que les permita reflejar no solo el estado de la respuesta a los ataques, sino su capacidad de reponerse de ellos. Que por medio de ellos se promueva la generación de bases de conocimiento que les permita a las empresas del sector no cometer los mismos errores y prepararse a las hostilidades de la red.

- El sistema de gestión debe contar con instrumentos como políticas, normas y procedimientos, entre otros, que le permita ser operativa. Estos deben responder a la criticidad de cada operación y deben permitir que su implementación siga un camino de madurez que permita una operación en ciberseguridad optimizada.

- Definir programas de auditoría que no se basen exclusivamente en métodos muestrales, sino que con una regularidad se pueda evaluar el estado completo de las redes TI y TO. Que estas auditorías les permitan a los gestores del sistema determinar las desviaciones y así, tomar las medidas que les permita encaminarse a la mejora continua.

- Las organizaciones deben definir con claridad al gobierno de la seguridad, iniciando por el CISO, designado con autoridad y mando para que pueda desempeñar sus funciones de manera dedicada y liderar todas las iniciativas para contar con una operación gobernable desde la ciberseguridad.

- Al contar con mecanismos de monitoreo alineado con los objetivos de ciberseguridad, se pueden disponer de indicadores de desempeño e indicadores de riesgo que les permita a los tomadores de decisión orientar sus esfuerzos manera eficaz y eficiente.

MANO DE OBRA

- Se debe promover la formación de los responsables de la seguridad siguiendo los esquemas de certificación internacional, esto pude incluir, certificación, especializaciones, maestrías y doctorados.

- Es importante promover en la alta dirección la formación, educación y entrenamiento en ciberseguridad y riesgos, de tal manera que les permita tomar decisiones basadas en datos.

- Promover la conformación en las empresas de CSIRT que reemplacen los SOC, dándoles la capacidad de responder rápidamente a los incidentes.

- Para aquellas organizaciones mucho más maduras, la conformación de RED y BLUE TEAMS que pongan a prueba su infraestructura.

MEDIO AMBIENTE

- Es importante promover la conformación de grupos sectoriales en cada país donde se comparta la información y las experiencias para resolver ataques.

- Promover la generación y participación en estudios multisectoriales en Latinoamérica y el Caribe en temas relacionados con la ciberseguridad.

MISIÓN

- La separación entre las redes es la mejor práctica que se está implementando, pero es necesario que vaya acompañado con políticas, normas, procesos y procedimientos que garanticen que solo los elementos que lo requieran se comuniquen entre sí.

- Toda necesidad de conectividad de la red TO debe responder a un exhaustivo ejercicio de riesgos, incluyendo la necesidad de conexión a Internet, que permita valorar las amenazas, las vulnerabilidades y las medidas de mitigación necesarias para no comprometer la operación.

- Es importante valorar que los dispositivos conectados en la red TO y que no son gestionados, pueden ser un vector de ataque. De igual manera las redes sombra, como la generada por dispositivos de almacenamiento USB, deben ser gestionadas y monitorizadas con rigor para evitar la transmisión de malware.

6.3.3 | Recomendaciones generales

A través del mismo modelo de gestión de riesgo de la sección anterior se presentan las siguientes conclusiones generales tanto para los formuladores de política como órganos rectores del sector eléctrico en América Latina y el Caribe.

MÁQUINA

- Se debe construir un esquema de gobernanza de la ciberseguridad en el sector, por medio de la articulación y armonización de las necesidades y requerimientos de las múltiples partes interesadas, bajo un marco institucional adecuado, con el fin de gestionar la ciberseguridad, bajo el liderazgo del Gobierno de cada país.

- Definir un marco legal y regulatorio que soporte todos los aspectos necesarios para adelantar la política.

MÉTODO

- Las múltiples partes interesadas del sector deben asumir la responsabilidad de la gestión del riesgo de ciberseguridad. Deben garantizar la rendición de cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás.

- Las organizaciones del sector deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de ciberseguridad.

- La gestión del riesgo debe llevarse a cabo de manera sistemática y continua, enfatizando en la evaluación de las posibles consecuencias de las amenazas y las vulnerabilidades en las infraestructuras

críticas asociadas. El tratamiento del riesgo debería tener como objetivo reducir el riesgo a un nivel aceptable en relación con los beneficios económicos y sociales.

- Con el objeto de reducir los efectos adversos de los incidentes de seguridad, y soportar la continuidad y la capacidad de recuperación de las actividades de las empresas del sector, deben adoptarse preparaciones y planes de continuidad. Los planes deben identificar las medidas para prevenir, detectar, responder y recuperarse de los incidentes y proporcionar mecanismos claros de escalamiento.

- Es necesario asegurar una responsabilidad compartida entre las múltiples partes interesadas, promoviendo la máxima colaboración y cooperación. Teniendo en cuenta el rol y el grado de responsabilidad de cada parte, para gestionar los riesgos de ciberseguridad y para proteger sus activos.

MANO DE OBRA

- Las partes interesadas deben buscar estar educados respecto a la gestión de la ciberseguridad, poseer las habilidades necesarias para entender el riesgo, administrarlo y evaluar su impacto.

- Los líderes y tomadores de decisiones deben asegurarse de que las medidas de seguridad sean apropiadas y proporcionales al riesgo, y deben tener en cuenta su potencial impacto, negativo o positivo, sobre las actividades del sector. La evaluación de riesgos de ciberseguridad debe guiar la selección, operación y mejora de las medidas de seguridad para llevar al riesgo a niveles aceptables.

- El estado debe promover una gestión sistemática y cíclica del riesgo de ciberseguridad, considerando el conjunto de iniciativas, procedimientos o metodologías coordinadas con el fin de abordar, de manera cíclica y holística, los riesgos de ciberseguridad en el sector.

MEDIO AMBIENTE

- Los líderes y tomadores de decisiones deben asegurarse de que la innovación sea considerada como parte integral de la reducción del riesgo de ciberseguridad. Esta debe fomentarse tanto en el diseño y funcionamiento de las arquitecturas y soluciones de la infraestructura crítica en el entorno digital, como en el diseño y el desarrollo de las medidas de seguridad.

MISIÓN

- El estado debe reconocer las múltiples partes interesadas y estas deben entender los riesgos de la ciberseguridad en el sector. Deben ser conscientes de que el riesgo de ciberseguridad puede afectar el logro de sus objetivos económicos y sociales.

- Se deben establecer los mecanismos para el fortalecimiento y construcción de capacidades humanas, técnicas, tecnológicas, operacionales y administrativas de las múltiples partes interesadas, que permita adelantar la gestión de riesgos de la ciberseguridad.

07 REFERENCIAS

[1]
NIST, «NIST Special Publication 800-39 Managing Information Security Risk Organization, Mission, and Information System View,» National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, 2011.

[2]
CDEC, «Estudio de diseño, especificación y programa la implementación del sistema de lectura remota de protecciones del sic y el sing,» 28 Diciembre 2016. [En línea]. Disponible en: https://sic.coordinador.cl/wp-content/uploads/2016/12/SLRP-A-Estado-del-Arte-y-B-Dise%C3%B1o-del-Sistema.pdf.

[3]
A. E. Motter y L. Ying-Cheng, «Cascade-based attacks on complex networks,» PHYSICAL REVIEW E, vol. 66, nº 1, p. 065102, 2002..

[4]
K. Lab, «The State of Industrial Cybersecurity 2018,» 2018.

[5]
CEER Council of European Energy Regulators , «CEER Cybersecurity Report on Europe's Electricity and Gas Sectors,» Bruselas, Bélgica, 2018.

[6]
The Public-Private Analytic Exchange Program, «Supply Chain Risks of SCADA/ Industrial Control Systemsin the Electricity Sector:Recognizing Risks and Recommended Mitigation Actions,» 2017. [En línea]. Disponible en: https://www.odni.gov/files/PE/Documents/11---Supply-Chain-Risks-of-SCADA-Industrial-Control-Systems-in-the-Electricity-Sector_Risks-and-Mitigations.pdf.

[7]
CCI Centro de Ciberseguridad Industrial, «LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y LA CIBERSEGURIDAD INDUSTRIAL,» 2013.

[8]
Trend Micro, «Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries,» 2018.

[9]
N. Huq, «Defensive Strategies for Industrial Control Systems,» 10 Enero 2017. [En línea]. Disponible en: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/defensive-strategies-for-industrial-control-systems.

[10]
CRITIFENCE Technologies Ltd., «CRITIFENCE,» 9 julio 2019. [En línea]. Disponible en: http://www.critifence.com/papers/attack-timeline/files/SCADA%20Cyber%20Attacks%20Timeline.pdf

[11]
E. Goldstein, «2018 CRITICAL INFRASTRUCTURE CYBER ATTACK TIMELINE,» 17 julio 2018. [En línea]. Disponible en: https://www.linkedin.com/pulse/2018-critical-infrastructure-cyber-attack-timeline-eran-goldstein.

[12]
A. Nagurney y D. Matsypura, «A Supply Chain Network Perspective for Electric PowerGeneration, Supply, Transmission, and Consumption,» Optimisation, Econometric and Financial Analysis, pp. 3-27, 2006.

[13]
WEF, «World Economic Forum. The Global Risk Report 2019.,» 2019. [En línea]. Available: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

[14]
N. Nhede, «Nhede, N. 2017. "Grid Automation Drives Increase in Utility Cybersecurity Investments: Report". Smart Energy International.,» 10 agosto 2017. [En línea]. Disponible en: https://www.smart-energy.com/industry-sectors/smart-grid/cybersecurity-technologies-navigant-research/.

[15]
OEA, «Resolución OEA AG/RES 2004 (XXXIV -0/04) Adopción de una Estrategia Interamericana,» 2004. [En línea]. Disponible en: https://www.sites.oas.org/cyber/Documents/Estrategia-seguridad-cibernetica-resolucion.pdf.

[16]
Parlamento Europeo, «Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,» 6 julio 2016. [En línea]. Disponible en: http://data.europa.eu/eli/dir/2016/1148/oj.

[17]
ENISA, «Appropriate security measures for smart grids. Guidelines to assess the siohisticatiion of security measures implementation,» 2012.

[18]
Energy.gov. 2020. Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). [En línea]. Disponible en: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-1→ [Accesado Diciembre 10 de 2019].