Presentación del estudio

El presente documento recoge un breve cuestionario (tiempo de respuesta estimado 20-30min) cuyo objetivo es la **recopilación de información sobre el nivel de preparación de su organización en materia de ciberseguridad.** Este cuestionario forma parte del estudio estadístico del nivel de madurez del tejido industrial de la Comunidad Valenciana realizado por el **Centro de Seguridad TIC de la Comunidad Valenciana (CSIRT-CV).** El CSIRT-CV es un organismo público sin ánimo de lucro cuyo objetivo es mejorar la ciberseguridad y promover una cultura cibersegura y buenas prácticas en las entidades públicas y privadas de la Comunidad Valenciana.

El estudio se ha iniciado en aras de obtener una imagen del nivel de preparación de las empresas industriales de la Comunidad Valenciana en materia de ciberseguridad industrial (para entornos OT) y está enfocado a la elaboración de un informe estadístico que presentará la información recogida de manera anonimizada.

Con el fin de que el estudio sea preciso y representativo, el cuestionario se ha dirigido a **personas que conozcan la organización de ciberseguridad en su organización**. No se requiere conocimiento técnico especializado para rellenarlo, pero sí sobre las medidas de seguridad implantadas y los procesos de gestión utilizados (de carácter general).

Ante cualquier duda sobre el estudio, o el mismo cuestionario, puede ponerse en contacto en:

CSIRT-CV - https://concienciat.gva.es/ - Correo: csirtcv_industrial@gva.es

Al final de este documento se incluye un breve **glosario de términos**, para su consulta en caso de dudas durante la cumplimentación del cuestionario.

Nota sobre el uso de los datos

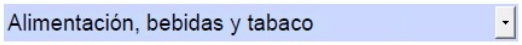
Rellenando este cuestionario accede a que se use la información recogida en él para fines estadísticos. La información recogida será tratada únicamente por el personal del CSIRT-CV autorizado para este fin y no será transmitida a terceros. En todo momento se aplicarán las medidas de seguridad necesarias para garantizar la privacidad de las empresas participantes en el estudio y la confidencialidad de la información aportada.

La información mostrada en el estudio final y en la difusión de sus resultados, se mantendrá anonimizada y será de carácter únicamente estadístico.

Instrucciones

1) Tipos de pregunta:

   a) Selección única. 

   b) Selección única mediante desplegable. 

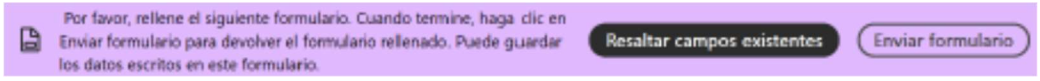
   c) Selección múltiple. 

   d) Respuesta abierta.

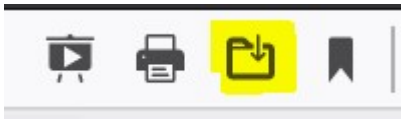
2) Rellene el formulario completo. Si no conoce la respuesta a una pregunta, o considera que no aplica en su organización, puede marcar la respuesta NS/NC en las preguntas de selección única, o no marcar ninguna respuesta en las de selección múltiple.

3) Algunas de las preguntas son secuenciales, lo cual quiere decir que sólo aplican si se ha respondido afirmativamente a la pregunta anterior. Dichas preguntas están agrupadas bajo un mismo número, con diferentes apartados (ejemplo 4a, 4b). En caso de que la primera respuesta sea negativa, no se tendrán que responder el resto de respuestas de los apartados posteriores. Dichos campos desaparecerán. Si cambia la opción inicial aparecerán de nuevo.

4) Se recomienda rellenar el formulario con Adobe Acrobat o los navegadores Chrome o Firefox. Por favor, siga los siguientes pasos para guardar y enviar el formulario completo.
   a) Adobe: una vez rellenado, seleccione el botón “Enviar formulario”, arriba a la derecha.



   b) Firefox y Chrome: una vez rellenado, seleccione el botón “Descargar”, arriba a la derecha. Envíe el archivo como adjunto en el correo.



   c) Explorer / Edge (no recomendado): una vez rellenado, seleccione el botón “Guardar”, arriba a la derecha. Envíe el archivo como adjunto en el correo.

Datos de la empresa

1. ¿Qué cargo ocupa en su empresa?

2. ¿Con cuántos empleados cuenta su compañía?

○ <10 ○ <50 ○ <250 ○ <500 ○ >500

3. ¿Cuál es el principal mercado de destino de los productos o servicios de su compañía?

○ Regional ○ Nacional ○ Unión Europea ○ Otros paises

4. ¿Cuál es la facturación global aproximada de su compañía?

○ <2 M ○ <10 M ○ <50 M ○ <200 M ○ >200 M ○ NS/NC

5. ¿En qué provincia de la Comunitat Valenciana tiene sede su compañía?

○ Castellón ○ Valencia ○ Alicante ○ Cuenta con sedes en varias provincias

6. ¿A qué sector pertenece la empresa?

NS/NC CNAE:

7. ¿Dispone su empresa de sistemas de control industrial para gestionar y controlar el proceso productivo? Marque los sistemas de los que dispone:

☐ Sistemas de control distribuido.
☐ Estaciones de operación, ordenadores industriales.
☐ SCADA´s, HMI´s.
☐ No se disponen de dispositivos industriales.
☐ Sistemas de control como PLC´s.

Auto evaluación previa

¿Cómo valoraría las siguientes afirmaciones respecto a su compañía? Siendo 1 totalmente en desacuerdo y 5 totalmente de acuerdo:

1. Nuestra organización cuenta con un nivel de madurez de ciberseguridad industrial avanzado.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ NS/NC

2. Los requisitos o demandas de ciberseguridad del sector (por parte de la competencia, clientes, proveedores y otros agentes) son muy exigentes.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ NS/NC

3. Es muy improbable que nuestra organización sufra un incidente de ciberseguridad de alto impacto en el próximo año.

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ NS/NC

Organización de la seguridad

1. ¿Se ha implementado una política de documentación interna que describe procesos y procedimientos de ciberseguridad?

- ◯ No.
- ◯ Sí, política interna de ciberseguridad o documento único director.
- ◯ Sí, procedimientos concretos para procesos de ciberseguridad específicos.

  (p.ej: Procedimientos de inventariado de archivos, accesos remotos, etc)
- ◯ NS/NC.

2a. ¿Se ha documentado en detalle las funciones de ciberseguridad en la empresa definiendo la responsabilidad de cada empleado o puesto de trabajo en cada una de dichas funciones?

◯ No ◯ Sí ◯ NS/NC

3. ¿Se han tenido que adaptar los procedimientos o medidas de ciberseguridad a las necesidades específicas de los entornos de producción (OT) de la empresa?

◯ No ◯ Sí ◯ NS/NC

4. ¿Se han implantado políticas o procedimientos de ciberseguridad para la gestión y uso de dispositivos portátiles y extraíbles (P.ej. ordenadores portátiles, móviles o memorias USB)?

◯ No ◯ Sí ◯ NS/NC

5a. ¿Se ha llevado a cabo algún tipo de evaluación de ciberseguridad en el entorno industrial?

- ☐ Ninguna evaluación.
- ☐ Evaluación organizativa (políticas, procedimientos).
- ☐ Evaluación técnica (segmentación, pentest).
- ☐ Evaluación Normativa (IEC62443-ISA99, LPIC,…).

6. ¿Se mantiene un inventario actualizado de los ciberactivos de la empresa? Se consideran todos los activos industriales como dispositivos electrónicos programables y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información.

- ○ No.
- ○ Sí, se actualiza tras cada cambio.
- ○ Sí, se actualiza periódicamente a intervalos fijos.
- ○ NS/NC.

7a. ¿Se han identificado e inventariado los activos críticos de la empresa? Se consideran activos críticos aquellos que, en caso de dejar de funcionar, detendrían todo el proceso productivo principal.

○ No ○ Sí ○ NS/NC

8. ¿Se han implementado políticas o procedimientos de seguridad para comprobar que no existen dispositivos o puertos accesibles desde internet?

○ No ○ Sí ○ NS/NC

Prevención

9a. ¿Se ha implantado un proceso de realización y gestión de copias de seguridad?

- ◯ No.
- ◯ Sí, pero no con una frecuencia establecida.
- ◯ Sí, se realizan copias de seguridad múltiples veces a la semana.
- ◯ NS/NC.

10. ¿Los ciber activos industriales cuentan con medidas de autenticación de usuarios? (p.ej: usuario/contraseña, autenticación doble factor, huella dactilar, reconocimiento facial, etc.).

- ◯ No.
- ◯ Sí, se ha protegido una parte de los activos.
- ◯ Sí, todos los activos cuentan con medidas de autenticación.
- ◯ NS/NC.

11. ¿Se han deshabilitado todas las cuentas de usuario por defecto, compartidas o genéricas (Por ejemplo usuarios "admin", "root", "mantenimiento"…)?

◯ No ◯ Sí ◯ NS/NC

12. ¿Se ha aplicado una política de contraseñas para el entorno industrial? Por ejemplo, la política debe de tener en cuenta aspectos como la robustez de las contraseñas (longitud, caracteres, etc), gestión de las contraseñas (cambio según una frecuencia temporal), eliminación de contraseñas por defecto.

○ No ○ Sí ○ NS/NC

13a. ¿La red interna corporativa (IT) está correctamente segmentada de la red industrial (OT)? Por ejemplo, los procesos productivos están segmentados o aislados de la red corporativa.

○ No ○ Sí ○ NS/NC

13c. ¿Es usual la utilización de routers inalámbricos para la conexión remota a los sistemas industriales?

○ No ○ Sí ○ NS/NC

14. ¿Se controla que la visibilidad y capacidad de actuación de los usuarios que accedan a la red depende de su rol y nivel de privilegios asignado?

○ No ○ Sí ○ NS/NC

15a. ¿Se permiten las conexiones remotas interactivas con ciber activos industriales?

○ No ○ Sí ○ NS/NC

16a. ¿Los ciber activos industriales disponen de un antivirus?

○ No ○ Sí ○ NS/NC

17. ¿Se han implantado soluciones alternativas para aquellos activos no compatibles con soluciones antivirus comerciales?

○ No ○ Sí ○ NS/NC

Personal y terceros

18a. ¿Qué empleados de la empresa reciben formación en materia de ciberseguridad?

- ○ No se imparte formación de ciberseguridad a ningún empleado.
- ○ Solamente los empleados con responsabilidades específicas de ciberseguridad.
- ○ Todos los empleados que trabajan directamente en procesos de producción.
- ○ Todos los empleados de la empresa.

19a. ¿Se exigen requisitos de ciberseguridad a proveedores y terceros, sobre productos o servicios? Por ejemplo, se deberían de definir cláusulas contractuales en materia de ciberseguridad y las responsabilidades por ambas partes.

- ◯ No
- ◯ Sí
- ◯ NS/NC

20. ¿Se ha contratado a terceros para funciones y procesos de ciberseguridad?

- ☐ No.
- ☐ Sí, para procesos de seguridad gestionada (Monitorización, respuesta a incidentes…).
- ☐ Sí, para evaluaciones de ciberseguridad.
- ☐ Sí, para funciones de formación o concienciación.
- ☐ Sí, para otras funciones (especifique).

Detección y respuesta

21a. ¿Qué tipo de medidas de monitorización de ciberseguridad se están utilizando sobre las redes industriales (OT)?

- ☐ Detección de malware.
- ☐ Detección de actividad sospechosa (IDS/IPS).
- ☐ Análisis de logs y generación de alarmas. (SIEM)
- ☐ Ninguna/No aplica.

22a. ¿Se han establecido planes de respuesta que incluyan información sobre cómo preparar, detectar, responder y recuperarse de incidentes de ciberseguridad?

○ No ○ Sí ○ NS/NC

23. ¿Se han implantado medidas para asegurar que la continuidad del proceso productivo no corra riesgo, en el caso de que exista alguna pérdida de recursos en la empresa que afecte a su actividad normal? (p. ej. instalaciones, activos redundantes, procesos de recuperación de los activos…).

○ No ○ Sí ○ NS/NC

24. ¿Existen procesos en la empresa para la gestión de vulnerabilidades y actualizaciones de los ciber activos? Por ejemplo, el testeo de las actualizaciones antes de su parcheado, la gestión y alerta de nuevas vulnerabilidades.

☐ No se ha implantado un procedimiento de gestión de vulnerabilidades y actualizaciones.

☐ Sí que existe una monitorización de nuevas vulnerabilidades.

☐ Se testean las actualizaciones antes de su implantación.

☐ La gestión de vulnerabilidades y actualizaciones de los sistemas es realizado por terceras partes.

25. ¿Existen activos en la empresa sin un mantenimiento activo de actualizaciones de seguridad o sin servicio técnico realizado por terceros?

○ No ○ Sí ○ NS/NC

Ampliación

26. ¿Se preveen realizar cambios y mejoras en la gestión de la ciberseguridad industrial de su empresa? Indicar cuál sería el motivo.

- ☐ Sí, por objetivos internos de mejora continua.
- ☐ Sí, por exigencias de normativas o estándares.
- ☐ Sí, debido a resultados de evaluaciones o análisis de riesgos.
- ☐ Sí, por exigencias del mercado o clientes.
- ☐ Sí, debido a experiencias pasadas en incidentes de ciberseguridad.
- ☐ Ninguna/No aplica.

27a. ¿Se prevé aumentar los recursos dedicados a la ciberseguridad industrial en su empresa en el próximo año?

○ No ○ Sí ○ NS/NC

28. ¿Se ha realizado o hay planes de realizar inversión en los próximos años en alguna de las siguientes tecnologías en la parte OT?

- ☐ Tecnología nube (p.ej. protocolo MQTT, AWS).
- ☐ IoT (Internet de las cosas)/ Smart Sensors/ Industria 4.0
- ☐ Tecnologías inalámbricas - wireless (p.ej. Zigbee, Lora).
- ☐ Inteligencia artificial y Machine learning.
- ☐ Big data.
- ☐ Gemelos digitales.
- ☐ Ninguna/No aplica.

29. Elija, de entre las siguientes, las normas y estándares relacionados con la ciberseguridad que se apliquen en su empresa:

- ☐ Controles Críticos de Seguridad (CSC).
- ☐ ISO 31000.
- ☐ ISO 22301 / BS 25999.
- ☐ ISO 27001.
- ☐ NIST 800-53.
- ☐ NIST 800-82.
- ☐ NERC CIP.
- ☐ Familia ISA 99 - IEC62443.
- ☐ Otras.
- ☐ Ninguna.

30. Ordene, de mayor a menor, según el peligro potencial que considere que estas amenazas presenten para su empresa: phishing, ransomware, malware o software malicioso, ataques a páginas/servicios web, personal interno malintencionado, espionaje industrial, APTs (Amenazas Persistentes Avanzadas), Vulnerabilidades de seguridad en activos, robo de credenciales.

Más peligroso	Malware o software malicioso	☐ NS/NC
	Malware o software malicioso	
	Malware o software malicioso	
	Malware o software malicioso	
	Malware o software malicioso	
	Malware o software malicioso	
	Malware o software malicioso	
	Malware o software malicioso	
Menos peligroso	Malware o software malicioso	

31a. ¿Ha experimentado su organización algún incidente de ciberseguridad que impactase el proceso industrial de la empresa en el último año (Parones de producción, retrasos, aumento de costes)?

- ◯ No.
- ◯ Sí, afectó solamente a los activos corporativos (IT).
- ◯ Sí, afectó solamente a los activos industriales (OT).
- ◯ Sí, afectó a activos IT y OT.
- ◯ NS/NC.

32. ¿Se ha detectado un aumento en los últimos 2 años del número de incidentes o ataques de ciberseguridad en su empresa?

◯ No ◯ Sí ◯ NS/NC

Respuesta abierta

RA1. Detalla la experiencia de la empresa ante el último incidente de ciberseguridad importante que haya sufrido su empresa. ¿Se colaboró con agentes externos? ¿Se cumplieron los planes de respuesta establecidos?

RA2. Tradicionalmente, en los procesos industriales no se han tenido en cuenta aspectos relacionados con la ciberseguridad industrial. Por esta razón, muchos de los protocolos usados en la actualidad no proporcionan ningún tipo de soporte en este ámbito.
Con el fin de identificar los más usados en nuestro tejido industrial, ¿podría indicar los protocolos y proveedores de componentes electrónicos más predominantes en su empresa?

Glosario

Activo crítico: Equipo o sistema esencial para mantener la operación de la empresa.

APT: Amenaza Persistente Avanzada. Grupo de atacantes con amplios recursos y conocimiento técnico, caracterizados por ataques a objetivos concretos que se extienden en largos periodos de tiempo.

Conexión remota interactiva: Comunicación con un activo ubicado en otra localización física que permite al usuario que se conecta actuar sobre el sistema como si lo estuviera usando directamente.

Copias de seguridad: Respaldo de información interna de la empresa almacenado de manera independiente con el objetivo de poder usarlo para restaurar los sistemas originales en caso de incidente.

Ciber activo: Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota.

Estaciones de operación: Lugares de trabajo con equipos de alto rendimiento destinados al trabajo técnico del operador.

Evaluación de ciberseguridad: Proceso por el cual se identifica el estado actual de un sistema, se compara con los objetivos de ciberseguridad de la organización y se identifican oportunidades de mejora.

Equipo proxy: Dispositivos que actúan de intermediarios entre redes o segmentos de red para redireccionar comunicaciones que no se desea que lleguen directamente a los equipos destino.

Firewall: Dispositivo o aplicación cuya función principal es bloquear comunicaciones entrantes y salientes no autorizadas de una red o segmento.

Gemelos digitales: Sistemas virtualizados que imitan, a algún nivel, el funcionamiento de un sistema real, para identificar comportamientos inesperados y evaluar hipótesis.

HMI: Interfaz interactiva visual entre trabajador y maquinaria industrial, habitualmente implementada en una tablet u ordenador pequeño.

IDS/IPS: Dispositivos o aplicaciones destinadas a monitorizar las comunicaciones de una red, detectar incidentes de seguridad y generar alarmas (IDS) o actuar para prevenir el riesgo (IPS).

IIoT: Industrial Internet of Things. Entornos OT donde se adoptan tecnologías IoT (sensores inteligentes, conexiones inalámbricas interactivas…) para aumentar la productividad o interacción con el sistema.

Incidente de ciberseguridad: Evento inesperado que conlleva una probabilidad de dañar o interrumpir la operativa habitual.

IT: Entornos donde predominan los activos y sistemas propios de las tecnologías de comunicaciones (P.ej. Una oficina, un equipo de ventas que trabaja en remoto…)

Medidas de autenticación: Controles de seguridad que verifican la identidad de los usuarios cuando intentan acceder al sistema.

Medidas de continuidad de negocio: Controles técnicos y administrativos orientados a asegurar las funciones esenciales de la empresa en caso de incidentes de alto impacto que puedan interrumpirlas.

Múltiples factores de autenticación: Medidas de autenticación que utilizan diversos controles, de diferente naturaleza, antes de autorizar a un usuario.

Nivel de madurez de ciberseguridad: Estado de preparación de una organización frente a riesgos de ciberseguridad potenciales, mediante medidas organizativas, procedimentales y técnicas.

Ordenadores industriales: Equipos diseñados para realizar labores industriales exigentes que no pueden llevarse a cabo por ordenadores comunes.

OT: Entornos donde predominan los activos y sistemas propios de procesos industriales (P.ej. una planta de producción industrial, un sistema de control SCADA…).

Phishing: Ataques donde el atacante suplanta a un agente o persona para ponerse en contacto con la víctima con la intención de robar información o ganar acceso a un sistema. La forma más habitual de esta amenaza es mediante correo electrónico.

Plan de respuesta: Procedimiento de actuación en caso de incidente de seguridad, que define roles y responsabilidades del equipo, así como medidas de seguridad y pasos a seguir para reducir el impacto del incidente y volver a la operativa habitual.

PLC: Controlador programable dedicado a la ejecución continua de la lógica de un proceso industrial.

Procedimiento de ciberseguridad: Documento interno que describe los pasos a seguir para llevar a cabo un proceso necesario para mantener la seguridad de la organización (P.ej. procedimiento de gestión de cambios, de gestión de usuarios y accesos…).

Protocolos industriales: Sistemas de comunicación usados por activos industriales para transmitirse información entre ellos (P.ej. Modbus, Profinet, OPC UA…).

Ransomware: Tipo específico de malware que cifra la información o equipos víctimas para interrumpir la operación o solicitar compensación económica de la víctima.

SCADA: Software de control, supervisión y adquisición de datos utilizado para monitorizar y actuar en tiempo real sobre un proceso productivo industrial.

Segmentación de red / segmentos de red: Separación de una red interna en zonas (segmentos o subredes) independientes, conectados entre sí solo por canales autorizados y protegidos para dejar pasar solamente las comunicaciones esenciales. Una segmentación habitual sería la separación de las redes IT y OT.

Seguridad perimetral: Medidas técnicas de seguridad implementadas para controlar las comunicaciones entrantes y salientes de una red o segmento de red.

Sistema de control distribuido (DCS): Hardware y software industrial dedicados al control de sistemas industriales. Se caracterizan por una base de datos central y capacidad de actuar en el resto del sistema y recibir información del resto del sistema.

VLAN: Dispositivos que redireccionan las comunicaciones entre activos para generar segmentos o subredes independientes.

Vulnerabilidad: Debilidad de seguridad técnica de un activo causada por fallos de diseño o desarrollo de nuevas técnicas de ataque, habitualmente solucionadas mediante la aplicación de actualizaciones de software o hardware.