CUATRO DILEMAS ESTRATÉGICOS DE CIBERSEGURIDAD INDUSTRIAL PARA DIRECTIVOS

José Valiente, Director de CCI

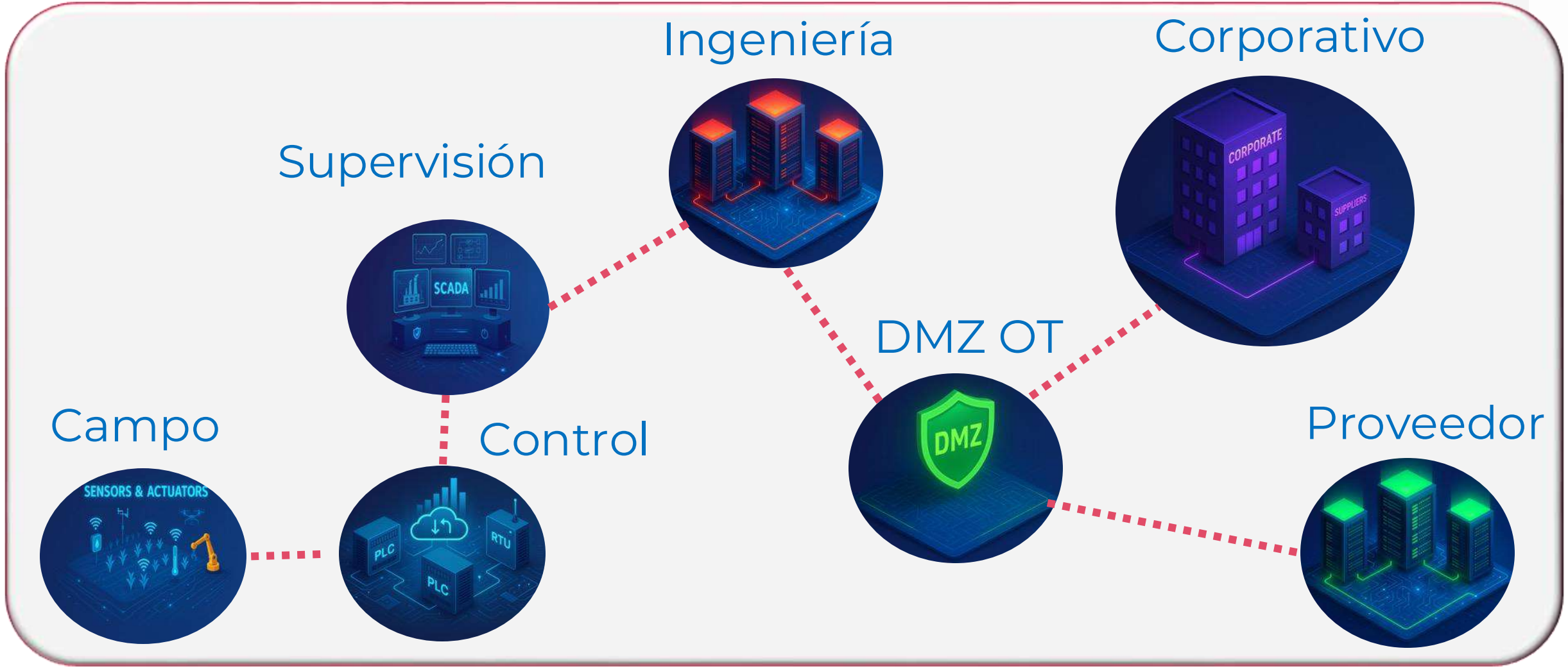
Herramienta

Equilibrio de Nash

www.cci-es.org

Centro de Ciberseguridad Industrial

Escenario de automatización Industrial



Metodología basada en el equilibrio de Nash

www.cci-es.org

DILEMA ESTRATÉGICO DE CIBERSEGURIDAD INDUSTRIAL

1

Escenario

Fabricante de automóviles detecta ransomware en SCADA.

Dilema: ***¿Restaurar lo antes posible? o ¿Revisar y aplicar medidas de ciberseguridad para contener y proteger aunque se detenga la producción más tiempo?***

Actores: CEO · Director de Producción · Director de Mantenimiento · Director de Ingeniería · Fabricantes OT· Regulador .

www.cci-es.org

1

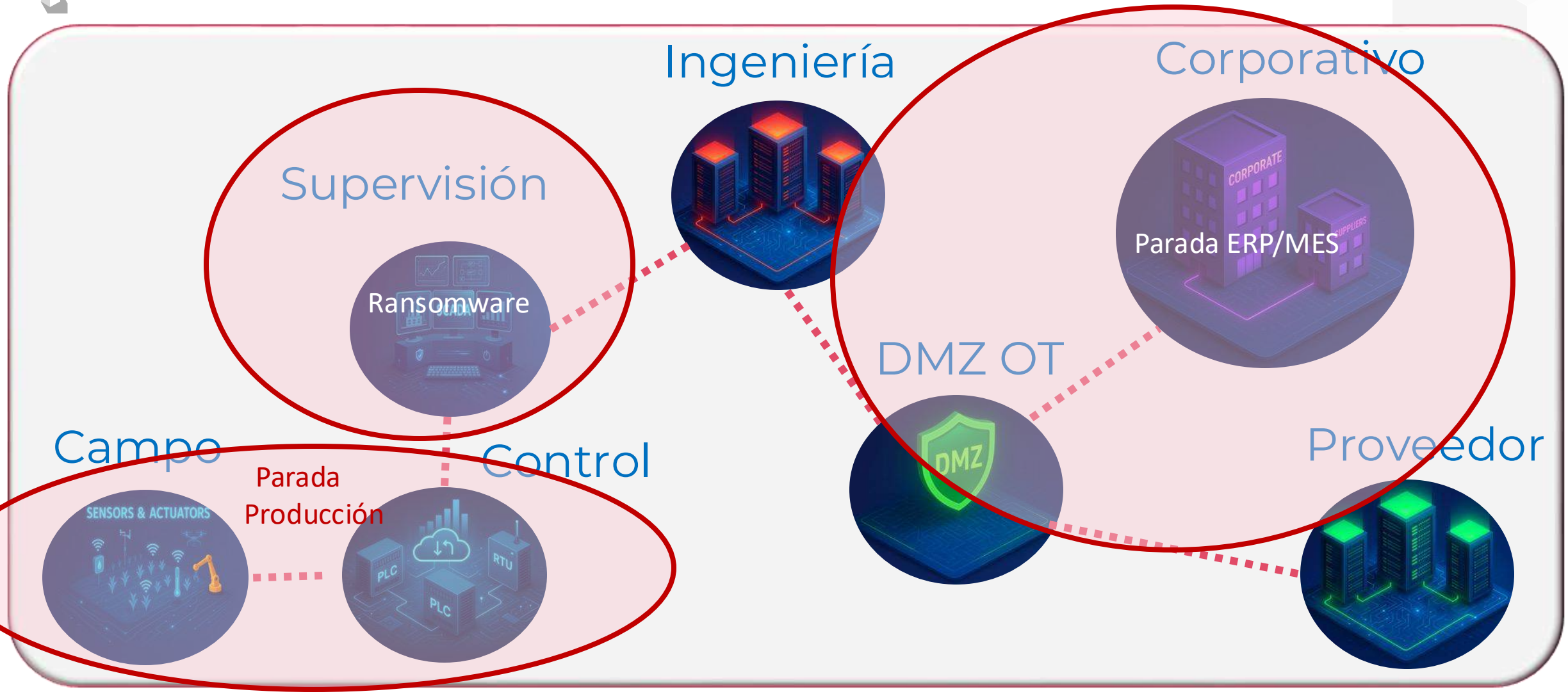
1. IDENTIFICAR EL PROBLEMA

¿Qué ha pasado? ¿Qué procesos están afectados? ¿Cuál es su impacto?

Un **Ransomware cifra servidores y HMI del SCADA** en una **planta de automoción**. La **integración con pedidos (MES/ERP)** queda interrumpida. La línea se para.

Centro de Ciberseguridad Industrial

Escenario de automatización Industrial



1

2. IDENTIFICAR ACTORES

¿Quiénes tomán decisiones, intervienen o se ven afectados?

Deciden: *CEO, Producción.*

Ejecutan: *Mantenimiento, Ingeniería, Fabricantes.*

Controlan cumplimiento: *Regulador.*

1

3. IDENTIFICAR CONTEXTO DE LOS ACTORES

¿Qué percibe cada actor? ¿Qué limitaciones tiene?

CEO: presión económica, reputacional y contractual.

Producción: presión en “arrancar ya”.

Mantenimiento: experiencia en averías físicas, poca práctica en ciber.

Ingeniería: aboga por contención y análisis forense.

Fabricante: necesidad de proteger su responsabilidad contractual; propone “restauración rápida” de su sistema.

Regulador: exige notificación y evidencia de control.

1

4. OBJETIVOS DE LOS ACTORES FRENTE A LA CRISIS

¿Qué busca cada uno en general en esta crisis?

CEO: *reducir impacto económico e impacto reputacional.*

Producción: *recuperar el ritmo diario (OEE).*

Mantenimiento: *restablecer disponibilidad con el mínimo riesgo.*

Ingeniería: *contener, erradicar, no re-infectarse.*

Fabricantes: *restaurar su plataforma conforme a contrato.*

Regulador: *transparencia y medidas proporcionales.*

1

5. EVALUAR RIESGOS Y OPORTUNIDADES

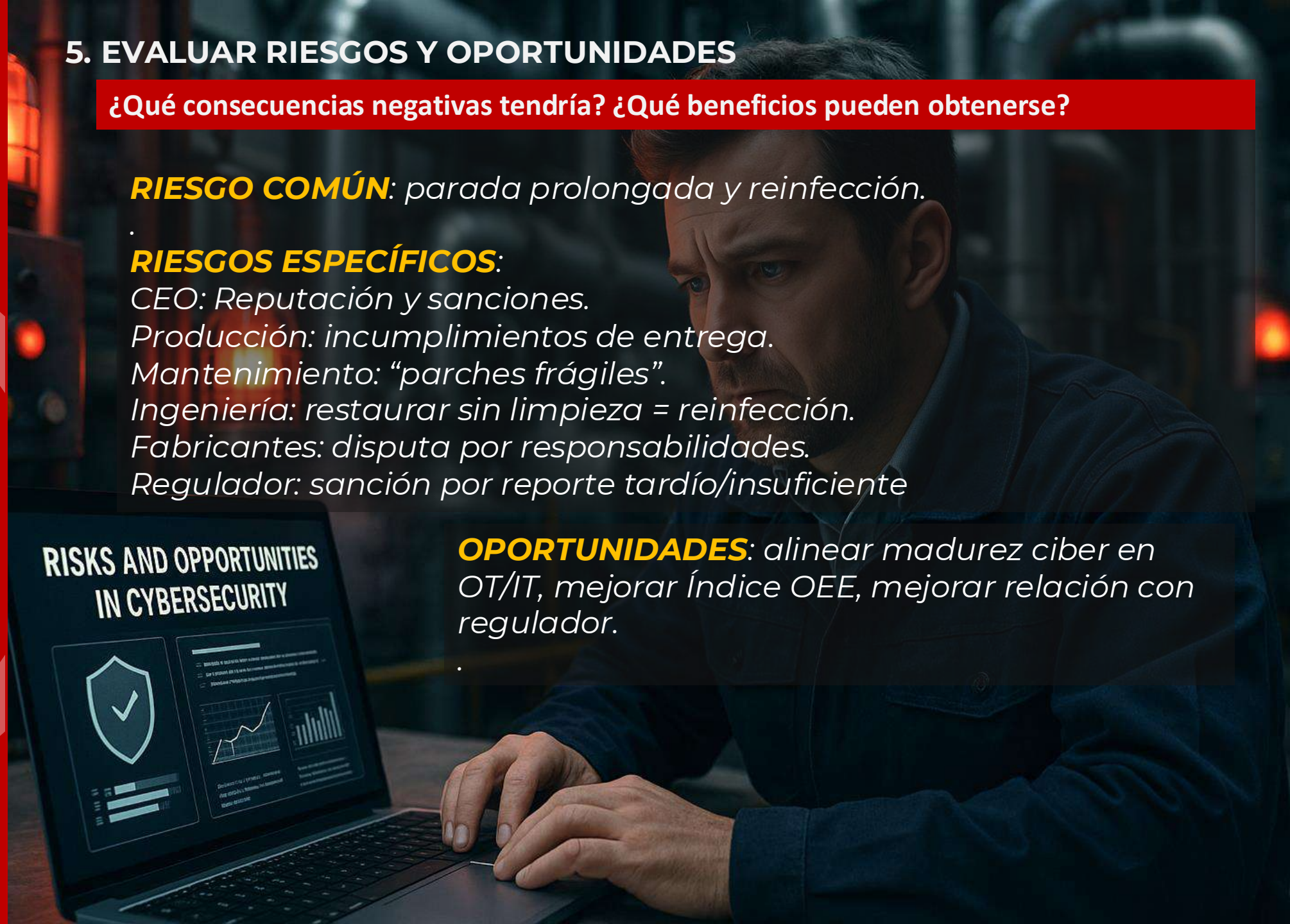
¿Qué consecuencias negativas tendría? ¿Qué beneficios pueden obtenerse?

RIESGO COMÚN: *parada prolongada y reinfección.*

.

RIESGOS ESPECÍFICOS:

CEO: Reputación y sanciones.
Producción: incumplimientos de entrega.
Mantenimiento: "parches frágiles".
Ingeniería: restaurar sin limpieza = reinfección.
Fabricantes: disputa por responsabilidades.
Regulador: sanción por reporte tardío/insuficiente



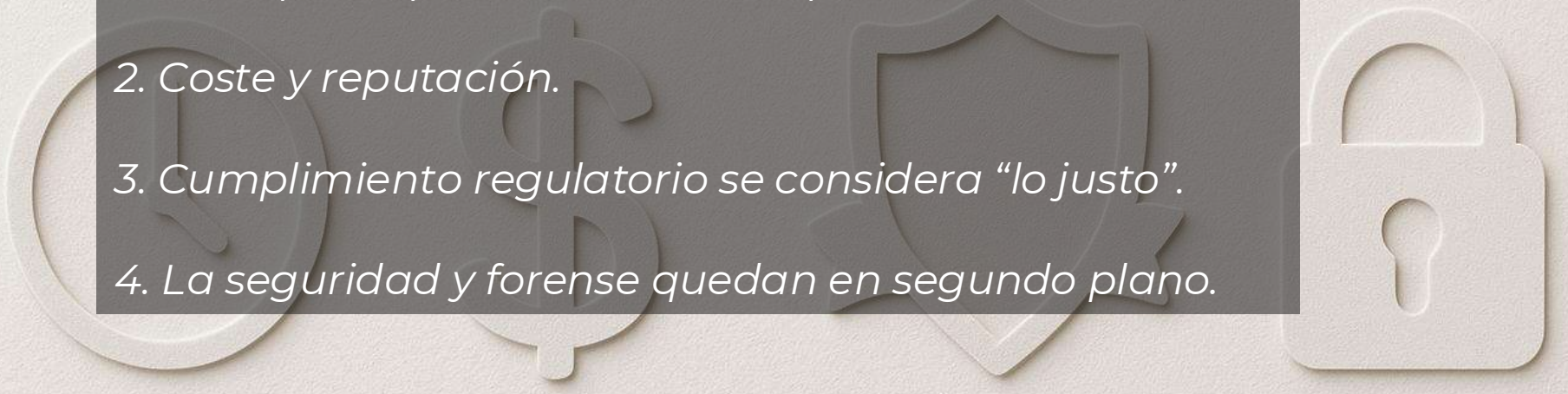
OPORTUNIDADES: *alinear madurez ciber en OT/IT, mejorar Índice OEE, mejorar relación con regulador.*

.

6. CRITERIOS PARA PRIORIZAR

¿Qué impacto pesa más: tiempo, coste, reputación, seguridad?

1. *Tiempo de parada domina la prioridad.*
2. *Coste y reputación.*
3. *Cumplimiento regulatorio se considera “lo justo”.*
4. *La seguridad y forense quedan en segundo plano.*



1

7. TIEMPO DE RESOLUCIÓN

¿Qué se puede resolver en corto, medio y largo plazo?

Corto (0–15 días): *se elige restaurar rápido desde copias no verificadas; se abren bypass entre IT/OT para colas de pedidos.*

Medio (1–6 meses*): se pospone segmentación y hardening "cuando pase la tormenta".*

Largo (>6 meses): *rediseño arquitectural indefinido, sin sponsor claro.*

Short Term

Medium Term

Long Term

8. SIMULAR ESCENARIOS

¿Qué pasa si cada actor va por libre?
¿Qué pasa si cooperan parcialmente?
¿Cuál es el punto donde nadie gana saliéndose del acuerdo?

A. Cada uno a lo suyo. *Producción manda arrancar; Fabricante restaura; Ingeniería sin tiempo para contención; Regulador informado tarde. Resultado: arranque en 3–4 días con alto riesgo residual.*

B. Cooperación parcial. *Se acuerda una "limpieza" mínima y comunicación limitada. Se reduce riesgo, pero quedan accesos temporales y credenciales sin cambiar.*

C. Cooperación plena (ideal). *Requiere facilitador o coordinador neutral y reglas claras (no existe ICSO): no se alcanza equilibrio.*

ICSO (Industrial Cybersecurity Officer)

DILEMA ESTRATÉGICO DE CIBERSEGURIDAD INDUSTRIAL

2

Mismo Escenario

Fabricante de automóviles detecta ransomware en SCADA, pero en la organización existe ya un ICSO (Responsable de ciberseguridad industrial)

2

DILEMA CON UN ROL ICSO

***ICSO**: El ICSO actúa como árbitro neutral en ciberseguridad, asegurando información compartida, objetivos alineados y equilibrio frente a presiones de producción y dirección.*

La cooperación entre áreas se establece antes y de manera más estable.
Producción** comprende que aceptar un retraso controlado reduce el riesgo de repetición de la incidencia**;
Ingeniería y Mantenimiento** cuentan con tiempo para aplicar medidas de contención y limpieza**;
el proveedor** recibe directrices claras que delimitan sus responsabilidades**;
***el regulador** es informado de forma proactiva, lo que genera confianza en la gestión.*

El resultado es una recuperación más rápida y segura, en la que los intereses de todos los actores se equilibran en un punto común.

2

DILEMA CON UN ROL ICSO

Antes del incidente

Prevención estructurada: El ICSO habría impulsado backups verificados, segmentación IT/OT y planes de respuesta.
Conciencia directiva: El CEO y Producción ya tendrían simulacros hechos → menos improvisación.
Relación con el regulador: Estaría anticipada, con canales de reporte preparados.

Durante el incidente

Coordinación centralizada: El ICSO actuaría como punto único de enlace entre CEO, Producción, Mantenimiento, Ingeniería y Fabricante.
Lenguaje común: Traduciría el problema técnico a impacto de negocio para el CEO y Producción, y viceversa.
Decisión más rápida: Menos conflicto entre "recuperar rápido" vs "recuperar seguro".

Después del incidente

Plan de acción en fases: Corto (restaurar), medio (reforzar), largo (rediseñar).
Lecciones aprendidas formalizadas: Documentación y mejora continua.
Confianza reforzada: Clientes y regulador perciben que la empresa tiene un responsable claro de la ciberseguridad industrial.

DILEMA ESTRATÉGICO DE CIBERSEGURIDAD INDUSTRIAL

3

Escenario

Fabricante de automóviles detecta vulnerabilidades en un proveedor crítico de software para sistemas OT.

Dilema: ***¿gestionar la relación en clave de suma cero (imponer requisitos y sanciones, aunque eso genere tensión y costes), o de suma positiva (colaborar, compartir conocimiento y elevar el nivel común de seguridad)?***

Actores: CEO · Director de Producción · Director de Mantenimiento · Director de Ingeniería · Fabricantes OT· Regulador · ICSO.

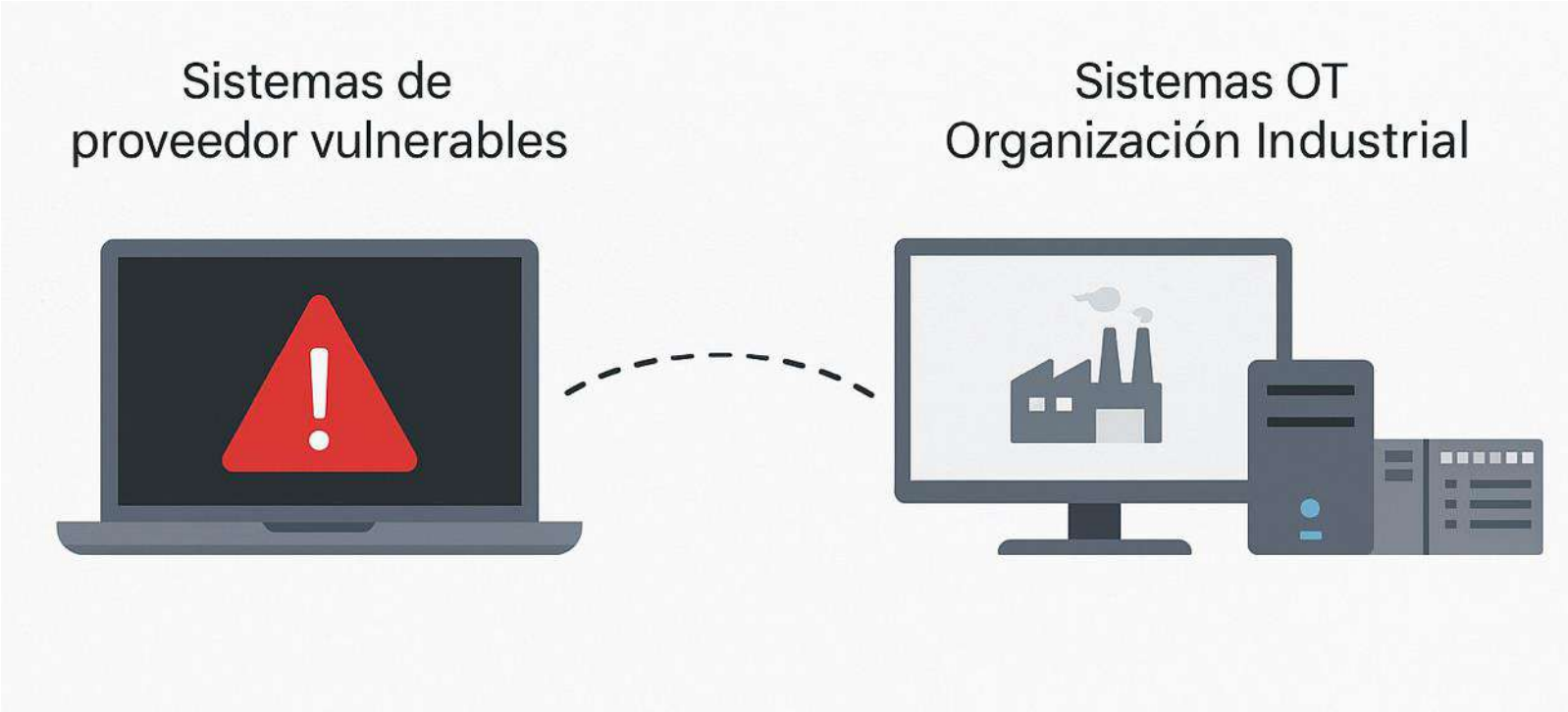
3

1. IDENTIFICAR EL PROBLEMA

¿Qué ha pasado? ¿Qué procesos están afectados? ¿Cuál es su impacto?

1. Detectada vulnerabilidad en software de un proveedor crítico.
2.De momento no hay sistemas afectados.
3. Riesgo: si no se resuelve, puede afectar la producción.

Decisión: ¿exigir al proveedor o cooperar con él?



3

2, 3 y 4. CARACTERIZAR ACTORES

¿Quiénes tomán decisiones, intervienen o se ven afectados?
¿Qué percibe cada actor? ¿Qué limitaciones tiene?
¿Qué busca cada uno en general en esta crisis?

CEO: *preocupado por clientes, reputación y contratos.*

Producción: *exige continuidad sin fallos. Piensa en el corto plazo (evitar paradas) y mantener entregas.*

Mantenimiento: *teme cargas extra si hay parches defectuosos. Busca evitar más carga por incidencias en cambios.*

Ingeniería: *quiere soluciones técnicas rápidas y robustas. Busca reforzar la seguridad técnica.*

Fabricante OT: *teme sanciones y pérdida de contrato. Quiere proteger su negocio y reputación. Busca no perder contrato.*

Regulador: *espera transparencia y reporting conforme a NIS2. Exige que se minimice el riesgo y se comunique. Busca cumplimiento normativo*

ICSO: *busca alinear intereses y guiar hacia un equilibrio estable. Percibe que el problema no es solo puntual, sino de madurez de ciberseguridad en la cadena de suministro. Su objetivo es lograr una estrategia equilibrada que reduzca el riesgo global.*

3

5. EVALUAR RIESGOS Y OPORTUNIDADES

¿Qué consecuencias negativas tendría? ¿Qué beneficios pueden obtenerse?

Riesgos de suma cero:
- *Ruptura de relación con proveedor.*
- *Costes y retrasos por sustituirlo.*
- *Reputación dañada por litigio.*

Riesgos de suma positiva:
- *Compartir información sensible.*
- *Necesidad de inversión conjunta.*

Oportunidades de suma cero:
- *Señal de firmeza a la cadena de suministro.*

Oportunidades de suma positiva:
- *Elevar el nivel de seguridad de toda la cadena.*
- *Fortalecer relación a largo plazo.*
- *Reducir riesgos sistémicos y ganar legitimidad ante regulador*

3

6. CRITERIOS PARA PRIORIZAR

¿Qué impacto pesa más: tiempo, coste, reputación, seguridad?

1. *Continuidad del negocio.*
2. *Reputación de la marca.*
3. *Cumplimiento regulatorio.*
4. *Coste económico.*
5. *Resiliencia a largo plazo.*

3

7. TIEMPO DE RESOLUCIÓN

¿Qué se puede resolver en corto, medio y largo plazo?

Corto plazo: *Identificación y categorización de proveedores.*

Medio plazo: *plan de colaboración con el proveedor (soporte, formación, auditorías, cláusulas contractuales de ciberseguridad).*

Largo plazo: *elevar requisitos a toda la cadena, crear un ecosistema sectorial más seguro y resliente.*

Short Term

Medium Term

Long Term

3

8. SIMULAR ESCENARIOS

¿Qué pasa si cada actor va por libre?
¿Qué pasa si cooperan parcialmente?
¿Cuál es el punto donde nadie gana saliéndose del acuerdo?

Escenario A (suma cero):
El fabricante sanciona al proveedor y amenaza con rescindir contrato. El proveedor oculta información para protegerse.

Resultado: desequilibrio, más desconfianza y riesgo sistémico.

Escenario B (suma positiva):
El fabricante, guiado por el ICSO, coopera con el proveedor, comparte buenas prácticas, involucra al regulador y refuerza contratos con cláusulas claras.

Resultado: mejora conjunta, confianza mutua y mayor resiliencia sectorial.

Simulaciones de Casos

DILEMA ESTRATÉGICO DE CIBERSEGURIDAD INDUSTRIAL

4

Escenario

Empresa industrial debe demostrar cumplimiento normativo de NIS2 (gestión de riesgos y cadena de suministro) y la CRA (seguridad de productos digitales y OT). Durante la preparación, se detecta que sus proveedores secundarios no cuentan con medidas básicas de ciberseguridad.

Dilema :¿Intentar resolver de manera aislada los requisitos de cumplimiento con recursos internos limitados? O ¿apoyarse en un ecosistema sectorial como el CCI, que aporta guías, plataformas, formación y redes de conocimiento para elevar el nivel de toda la cadena?

01

IDENTIFICAR EL PROBLEMA

Riesgo de incumplimiento regulatorio (NIS2 / CRA) en la cadena de suministro.
Impacto: sanciones económicas, pérdida de contratos y reputación.

02

IDENTIFICAR ACTORES

Internos: CEO, Producción, Mantenimiento, Ingeniería, ICSO.
Externos: Proveedores, Regulador, CCI como recurso de apoyo.

03

CONTEXTO Y OBJETIVOS

CEO: presión de consejo y regulador.
Producción: riesgo de interrupción.
Proveedores: sin madurez ni recursos.
Regulador: exige evidencias claras.
ICSO: busca un marco ordenado.
CCI: ofrece guías, plataformas y formación como apoyo inmediato.

04

EVALUAR RIESGOS Y OPORTUNIDADES

Riesgos de actuar solo: costes altos, duplicación de esfuerzos, incumplimientos.
Oportunidades con CCI: usar guías como SGCI, el Rincón del Compliance, plataformas RECIN/ESCIM/MACIN para estructurar evidencias, y la Escuela para capacitar a empleados y proveedores.

05

TIEMPO DE RESOLUCIÓN

Corto plazo: aplicar SGCI y el Rincón del Compliance para ordenar requisitos y reporting.
Medio plazo: usar plataformas CCI para estructurar la evaluación de proveedores.
Largo plazo: formar a la cadena a través de la Escuela y los equipos de conocimiento.

06

SIMULAR ESCENARIOS

A (aislado): la empresa trata de imponer requisitos por su cuenta → incumplimientos parciales, proveedores tensos, riesgo de sanción.
B (con CCI): el ICSO usa guías y plataformas del CCI, forma a proveedores y reporta al regulador con evidencias sectoriales → cumplimiento sólido, confianza del regulador y resiliencia compartida.

5 principios rectores de las decisiones estratégicas

PRINCIPIO	QUÉ SIGNIFICA EN LA PRÁCTICA	EJEMPLO EN CIBERINCIDENTE INDUSTRIAL
Transparencia	Informar de manera clara y completa a actores internos y externos relevantes.	Comunicar al regulador de forma proactiva el alcance del ataque y las medidas tomadas.
Resiliencia	No limitarse a restaurar, sino reforzar la capacidad futura de respuesta.	Aprovechar la crisis para segmentar redes y validar copias de seguridad.
Cooperación	Implicar a todas las áreas y proveedores en una estrategia común.	Reunir en una mesa al CEO, Producción, Ingeniería, Mantenimiento y Vendor para consensuar acciones.
Proporcionalidad	Tomar medidas equilibradas entre coste, urgencia e impacto.	Reanudar producción con controles adecuados en el nivel oportuno.
Aprendizaje	Convertir el incidente en una oportunidad de mejora continua.	Documentar el caso, extraer lecciones y preparar simulaciones internas con lo aprendido.

SOLICITAR GUÍA

www.cci-es.org

Centro de Ciberseguridad Industrial

www.CCI-es.org