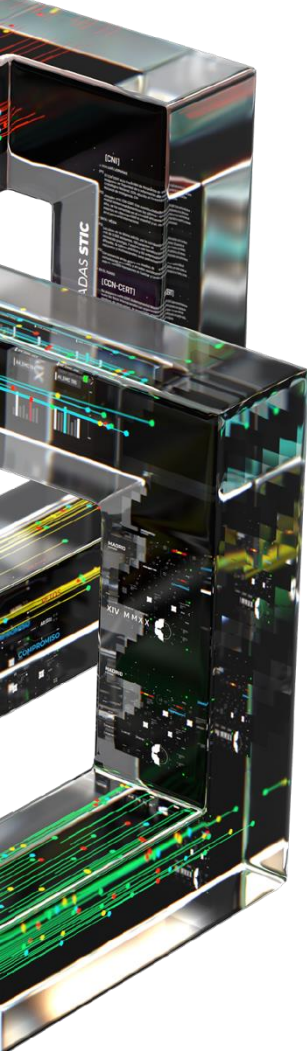
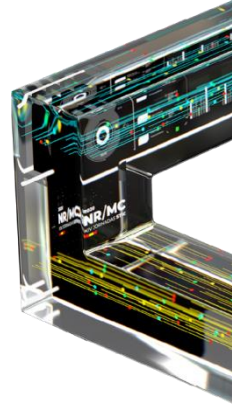




#XIVJORNADASCCNCERT

Retos en Gestión de Ciber Incidentes en Entornos Industriales





Agustin Valencia Gil-Ortega

 **IBERDROLA** *Head Of Global OT Cybersecurity*

 **CCI – Centro Ciberseguridad Industrial**

<https://www.linkedin.com/in/agustinvalencia/>

Gestión de Grandes Incidentes

Impacto

- ✓ Impacto a la Población
- ✓ Impacto al medioambiente
- ✓ Impacto a los trabajadores
- ✓ Impacto a las Instalaciones
- ✓ Impacto Reputacional

Ley PIC 8/2011 – RD 704/2011

Guía Notificación y Gestión de ciberincidentes (9 enero 2019)



Gestión de Grandes Incidentes

Seveso (1976) Italia

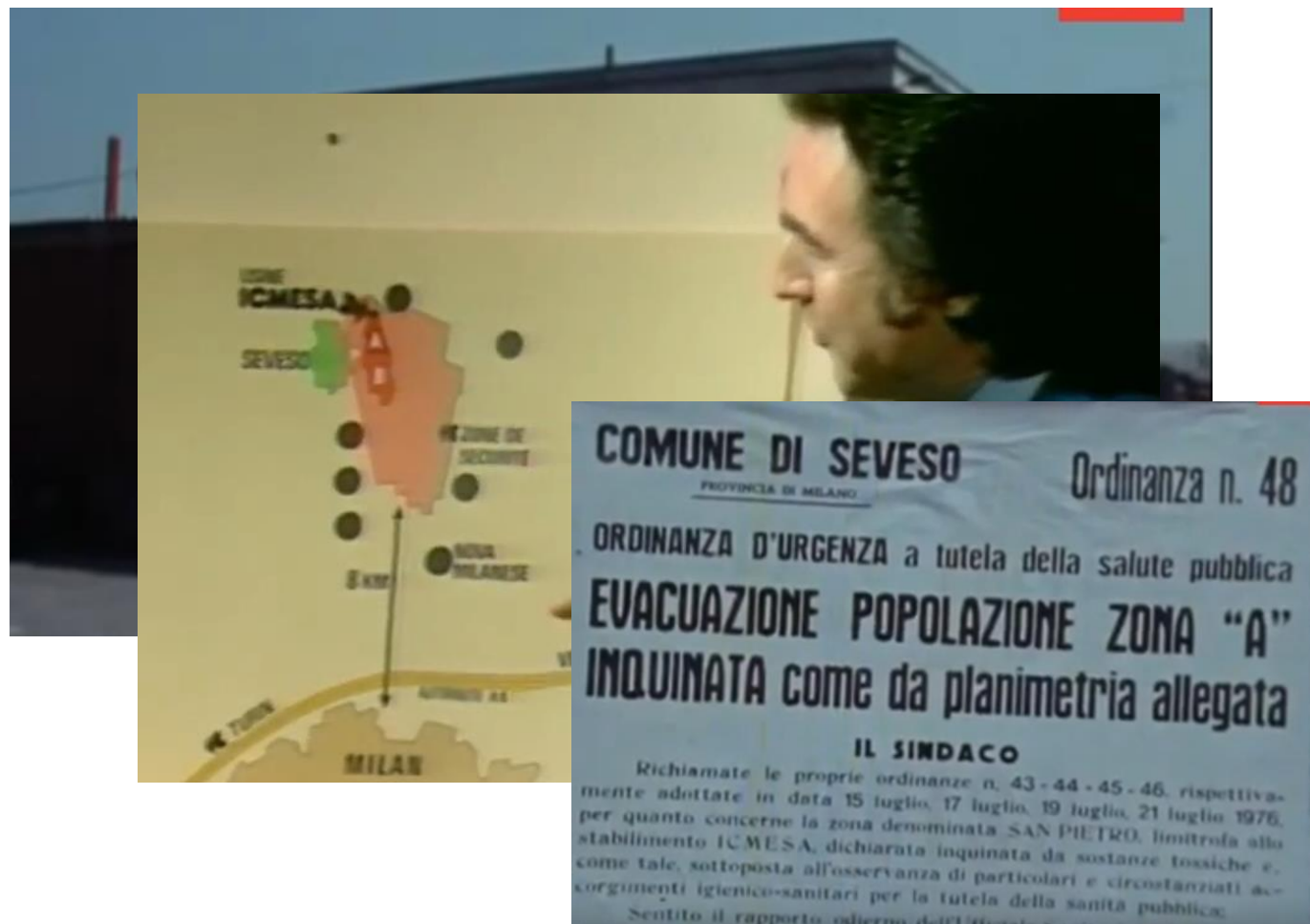
Escape de Gases Tóxicos (TCDD)

Sin mecanismos de alerta

Evacuación 733 personas

Muerte de animales y enfermedades de personas (5000)

- ➔ Inicio de legislación de seguridad industrial
- ➔ Directiva 82/501/CEE del Consejo, de 24 de junio de 1982



Gestión de Grandes Incidentes

Three Mile Island TMI-2 (28-3-1979) Harrisburg, PA, USA

Fallo Humano por instrumentación insuficiente → Fusión del reactor

Radiación en áreas de la planta → Supervisor declara emergencia general

Baja radiación al exterior

Portavoces no preparados

Película “El síndrome de China” estrenada 12 días antes

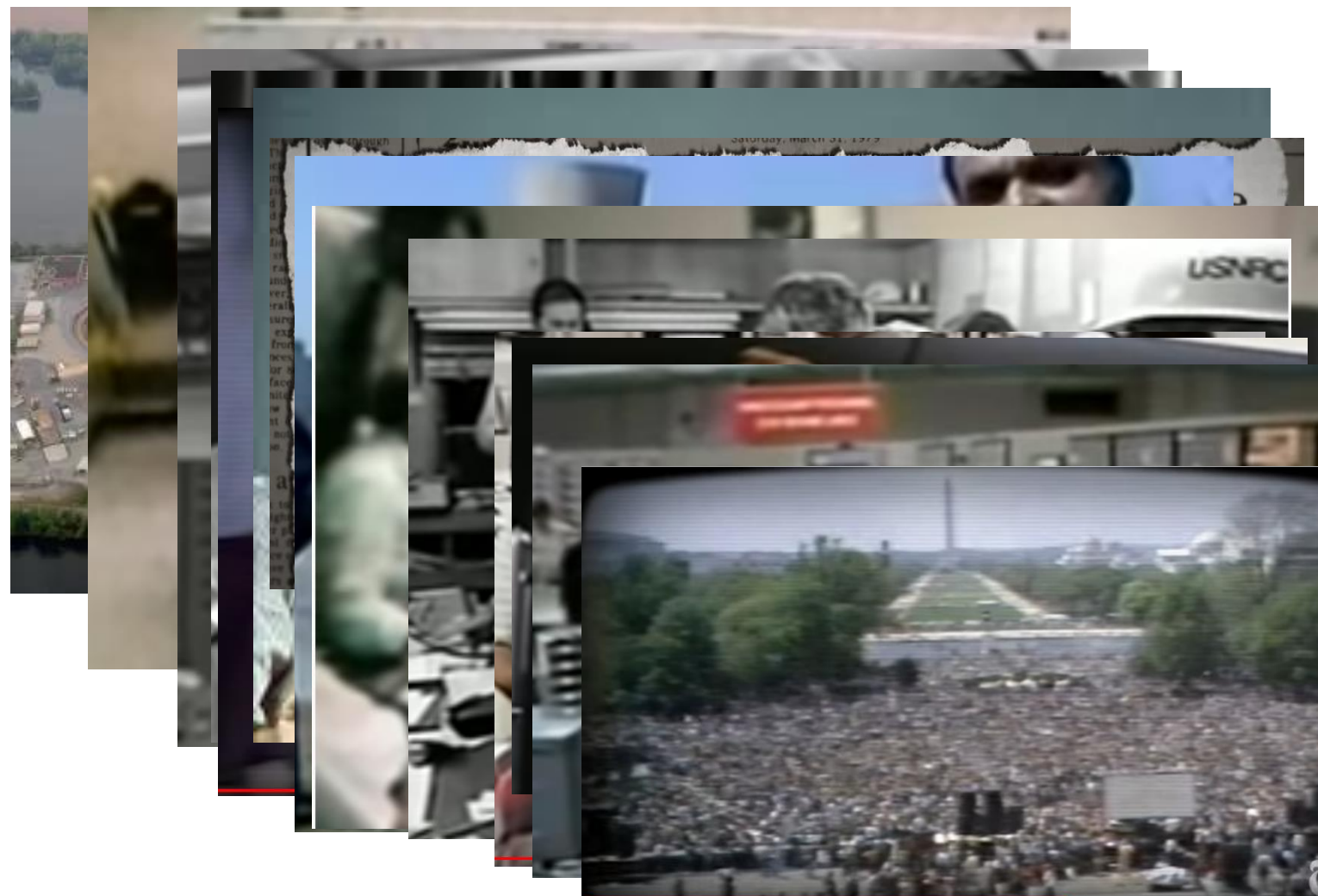
Caos de Población y Medios

Sala de control desbordada

1 abril el Presidente se persona

Auge Movimiento antinuclear

#XIVJORNADASCNCERT



Gestión de Grandes Incidentes

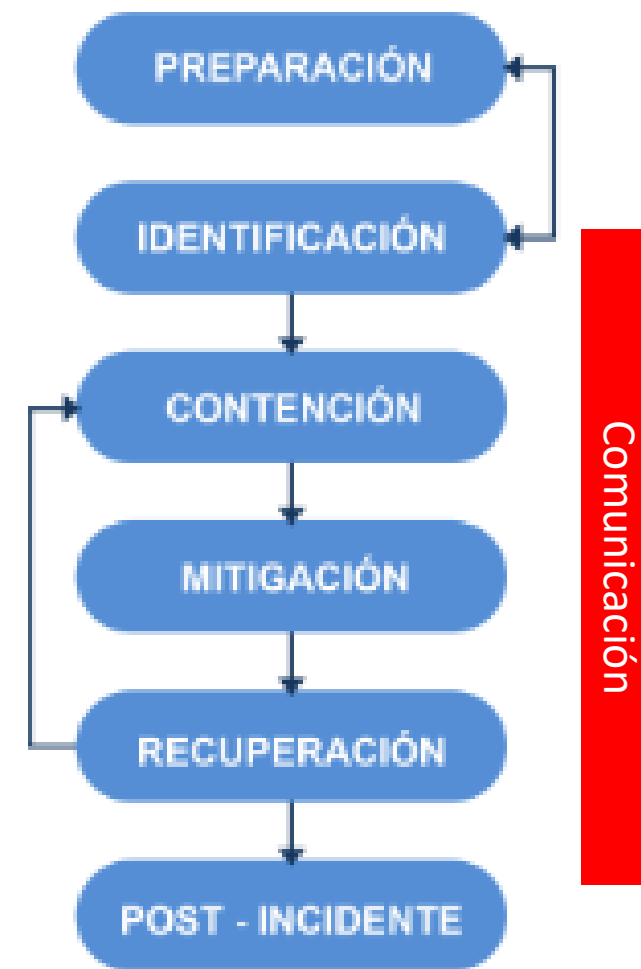
Ciberincidentes → Similitudes!!

- ✓ Hay definidos mecanismos de comunicación al regulador
- ✓ Avalancha de trabajo → disciplinas técnicas, seguridad, emergencias
- ✓ Necesidad de tener claro quién dirige las acciones internamente
- ✓ Necesidad de coordinar acciones con otras organizaciones
- ✓ Necesidad de gestionar el incidente externamente
- ✓ Complejidad en describir los hechos a los medios
- ✓ Preocupación de la sociedad hacia consecuencias inimaginables
- ✓ Todos quieren saber qué pasa → Colapso de comunicaciones?

Gestión de Grandes Incidentes

A tener en cuenta → COMUNICACIÓN

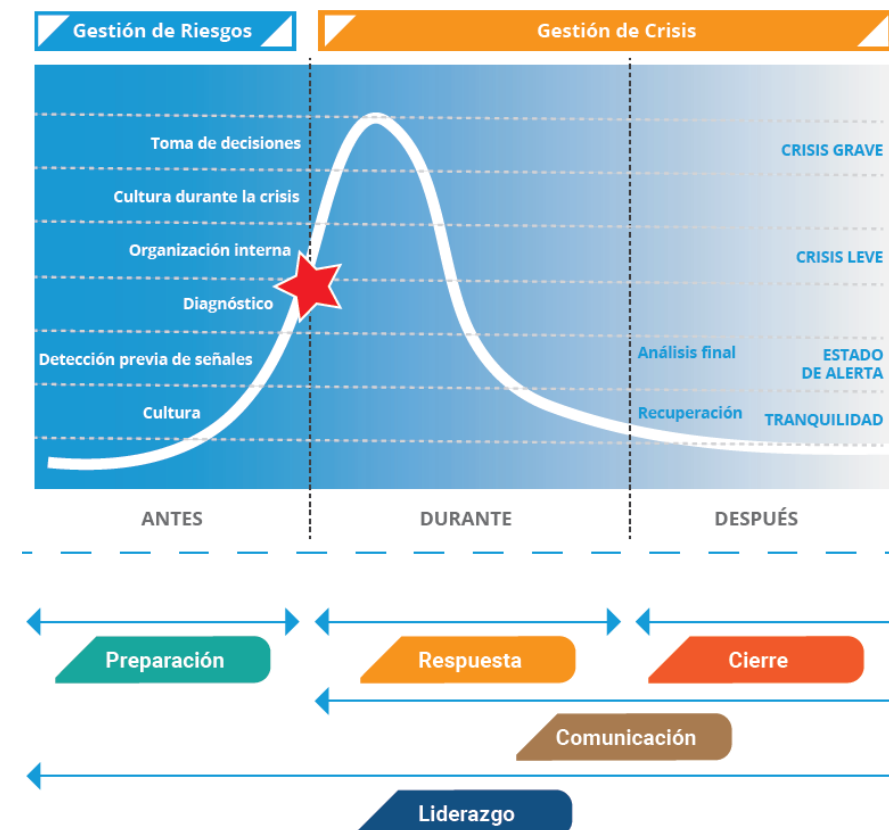
- ✓ Efecto multiplicador de las RRSS
- ✓ Ciberataques aprovechando ciber incidentes?
- ✓ Intentos de desinformación desde RRSS??
- ✓ Quién lidera la comunicación?
 - ✓ Credibilidad, claridad, concreción
 - ✓ Comunicadores identificables desde organizaciones



Gestión de Grandes Incidentes

ORGANIZACIÓN

✓ *¿Cómo están las organizaciones industriales?*



➔ *Consulta Ecosistema CCI*

BUENAS PRÁCTICAS EN LA GESTIÓN DE CRISIS DE CIBERSEGURIDAD BP-20 Octubre 2020

Gestión de Grandes Incidentes

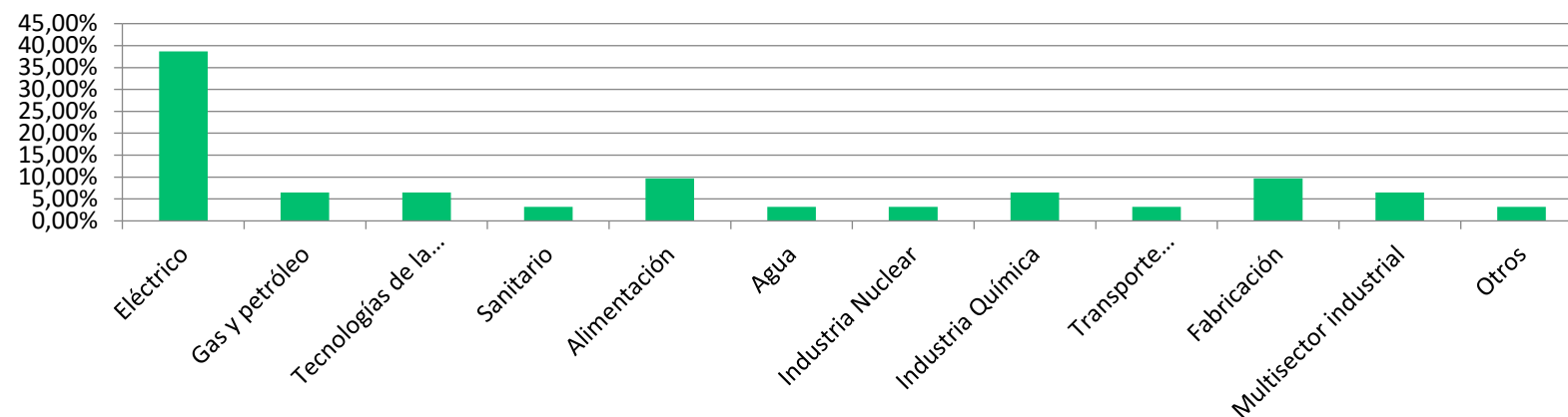
ECOSISTEMA CONSULTADO (España + LATAM)



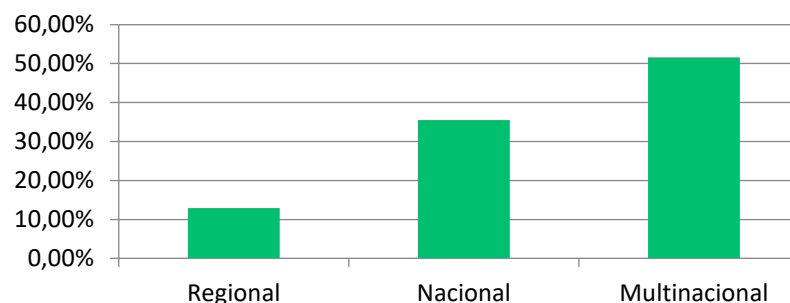
✓ 1ª Respuesta

- ✓ 31 respuestas
- ✓ Informe completo 2021

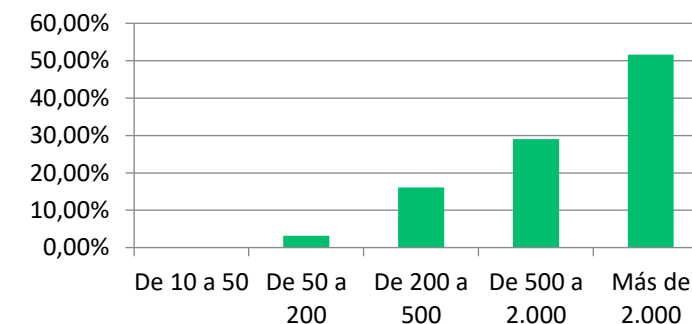
Sector de la organización a la que representa



Alcance Geográfico



Número de empleados

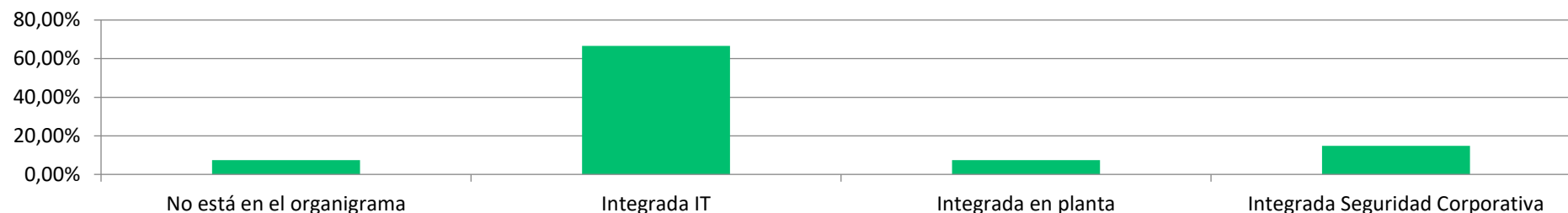


Gestión de Grandes Incidentes

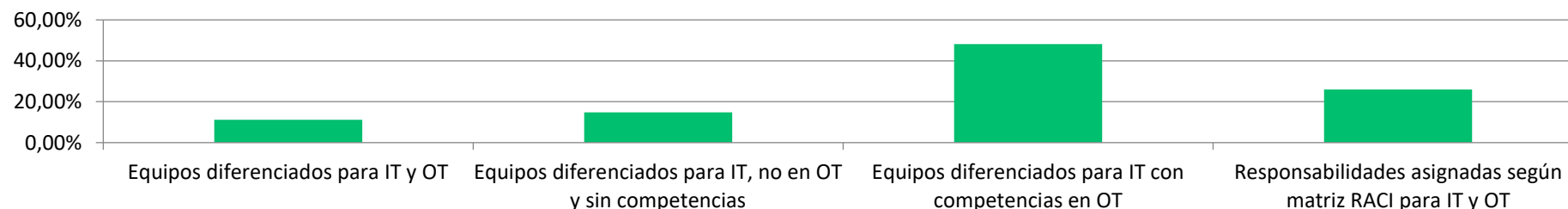
ECOSISTEMA CONSULTADO – ORGANIZACIÓN CIBERSEGURIDAD

✓ Como responde la organización ante grandes ciber incidentes

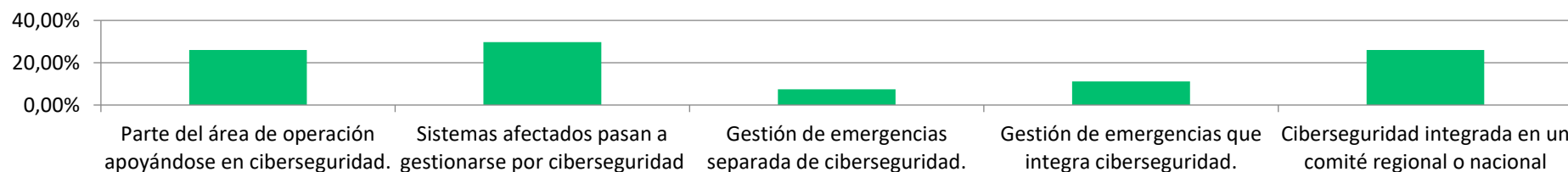
¿Cuál es la posición de ciberseguridad en su estructura organizativa?



¿Cuál es la distribución de roles y responsabilidades en la ciberseguridad en su organización?



¿Cómo es la gestión de emergencias de un incidente de ciberseguridad de alto impacto?

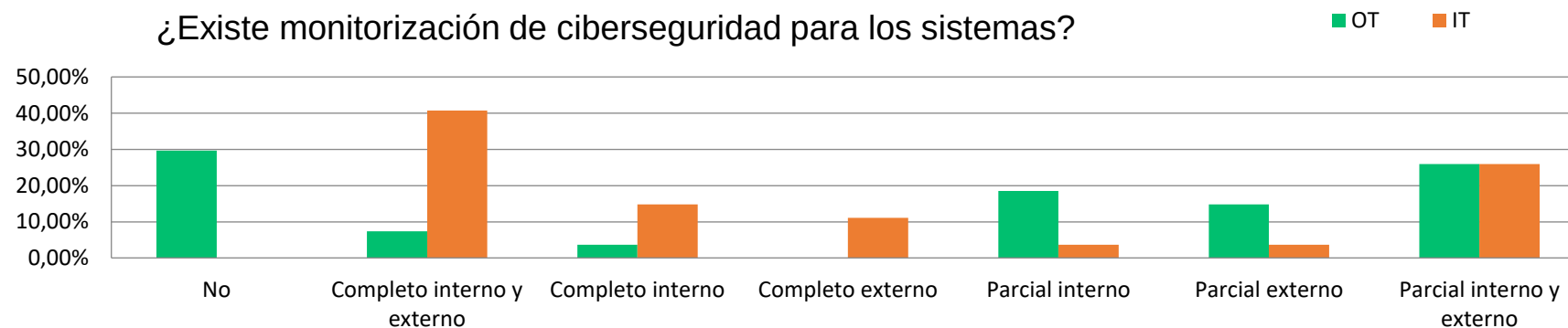


Gestión de Grandes Incidentes

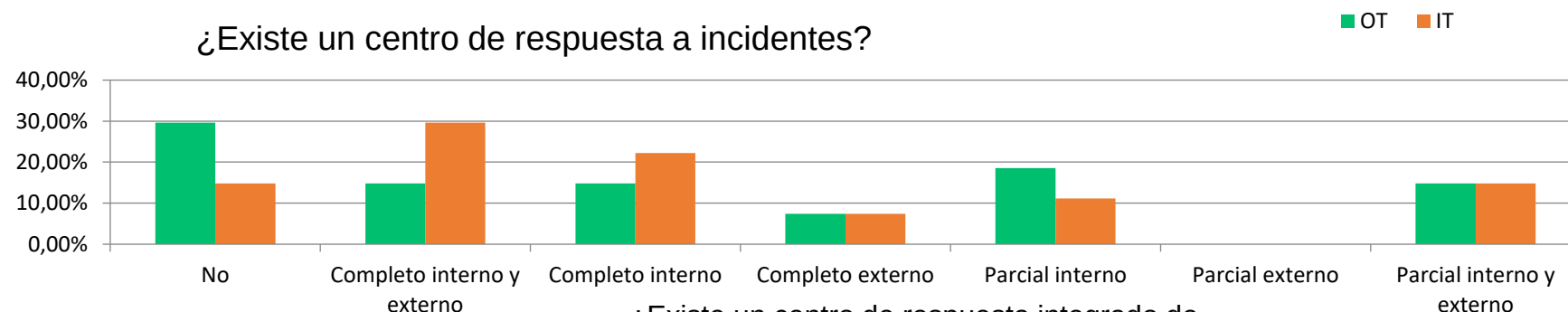
ECOSISTEMA CONSULTADO – CAPACIDADES TÉCNICAS



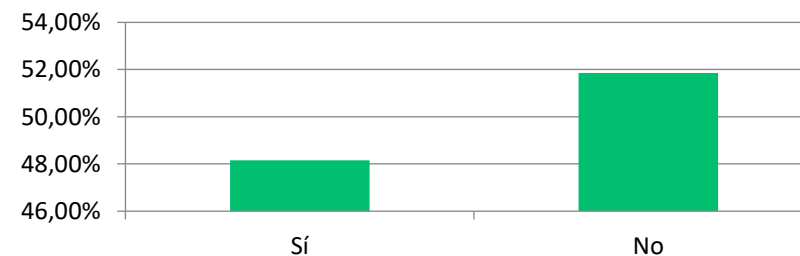
¿Existe monitorización de ciberseguridad para los sistemas?



¿Existe un centro de respuesta a incidentes?



¿Existe un centro de respuesta integrado de sistemas de información y operación?

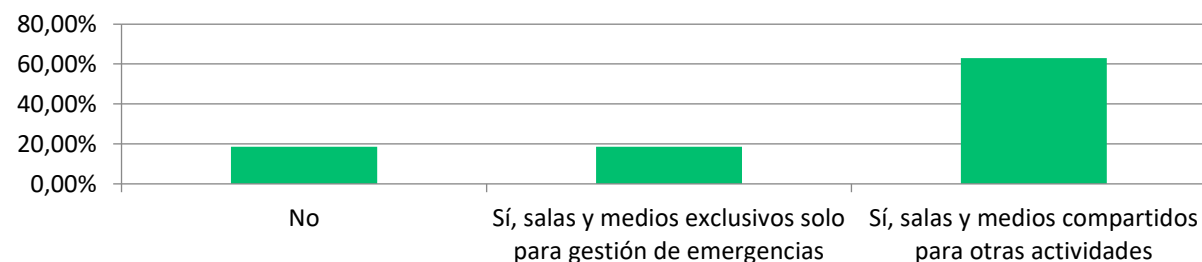


Gestión de Grandes Incidentes

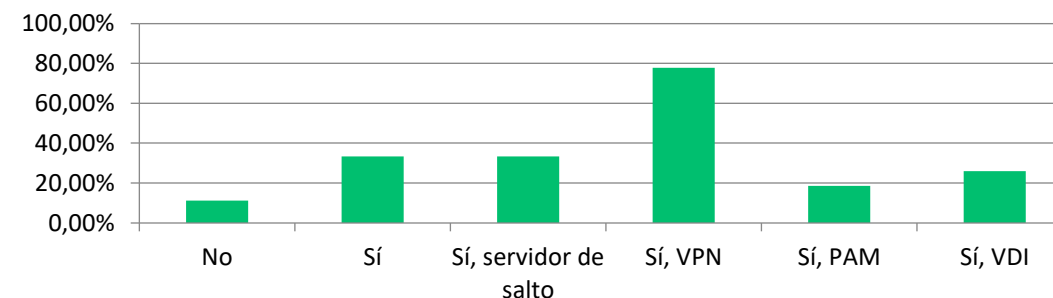
ECOSISTEMA CONSULTADO – CAPACIDADES TÉCNICAS

PREPARACIÓN

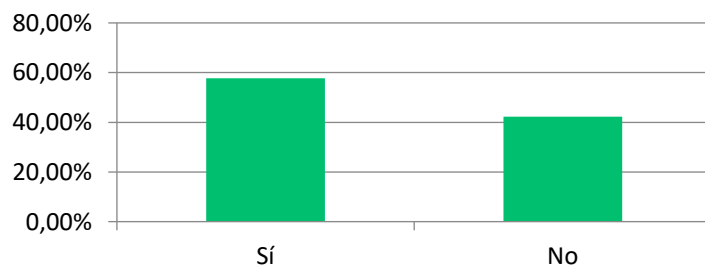
¿Existen salas y medios de telecomunicaciones habilitados para la gestión de emergencias?



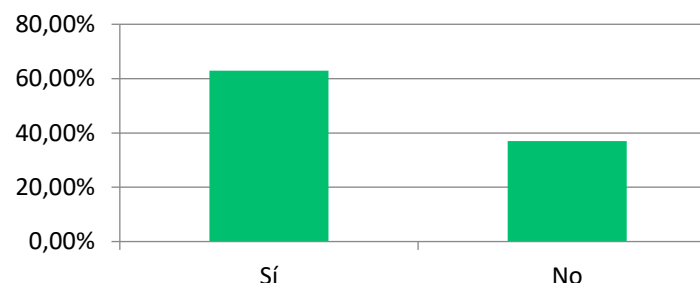
¿Existe capacidad de acceso de terceros a una red comprometida para solventar un incidente de ciberseguridad de alto impacto?



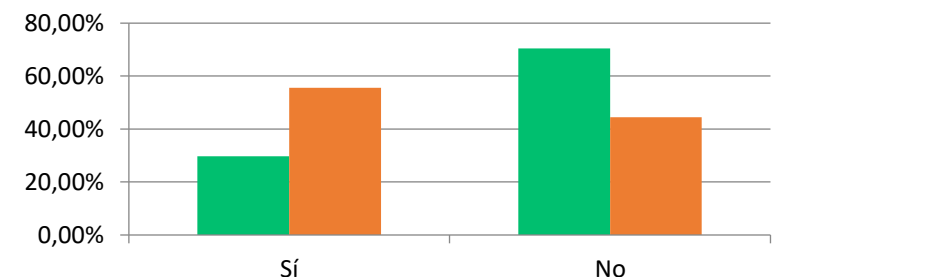
¿Existe capacidad de análisis forense mediante la monitorización de red?



¿Existe capacidad de acceso de extracción de muestras de sistemas de supervisión (SCADA, HMI...)?



¿Existen capacidades de análisis forense de ciberseguridad en los sistemas de infraestructuras industriales?

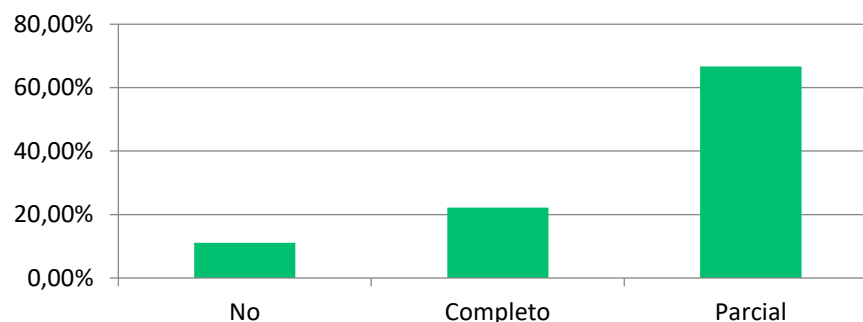


Gestión de Grandes Incidentes

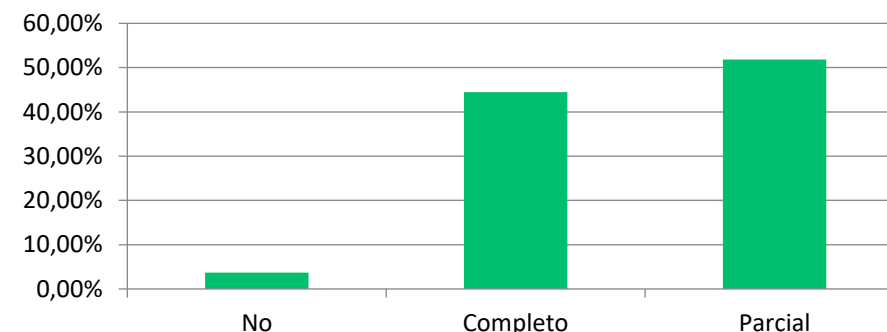
ECOSISTEMA CONSULTADO – PROCEDIMIENTOS

COORDINACIÓN

¿Existe en el centro de control protocolos para activar el área/organización de emergencia, indicando quienes son los responsables y roles en las plantas industriales?

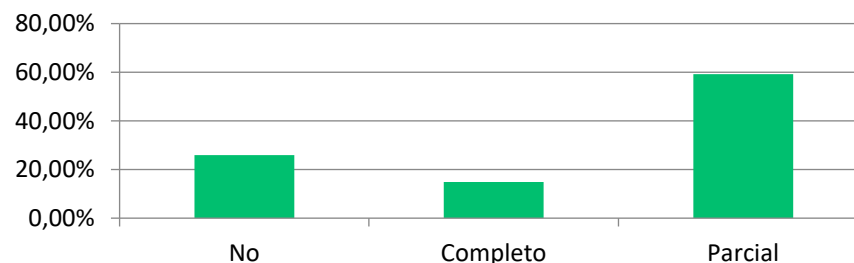


¿Existen a nivel corporativo protocolos para activar área/organizaciones de emergencia, indicando quienes son los responsables y roles?

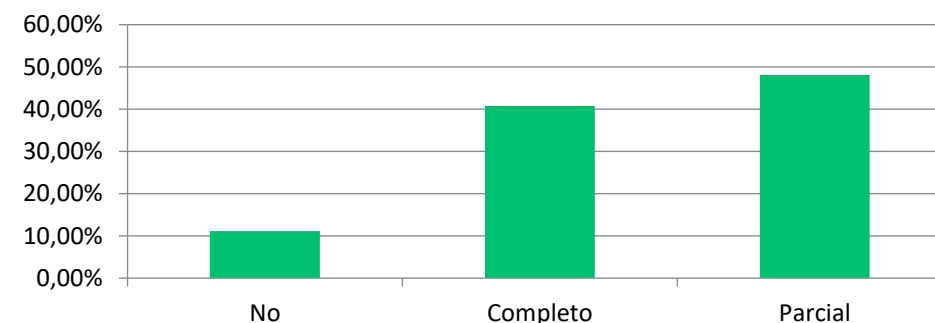


COMUNICACIÓN

¿El personal de operación en centros de control tiene protocolos de actuación para identificar ciberataques, avisar tanto internamente, como a terceros (reguladores,...)?



¿Existen protocolos para informar a medios de comunicación indicando portavoces, contactos internos y externos de la organización?

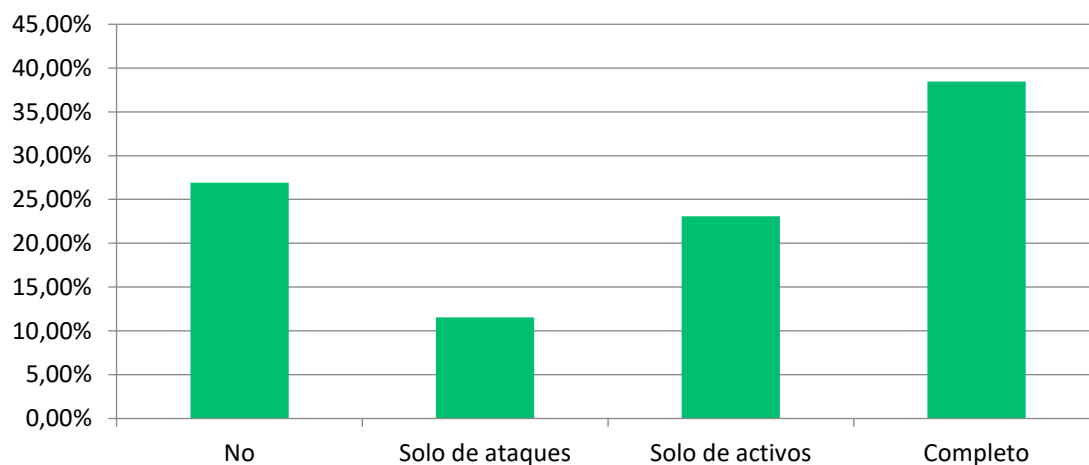


Gestión de Grandes Incidentes

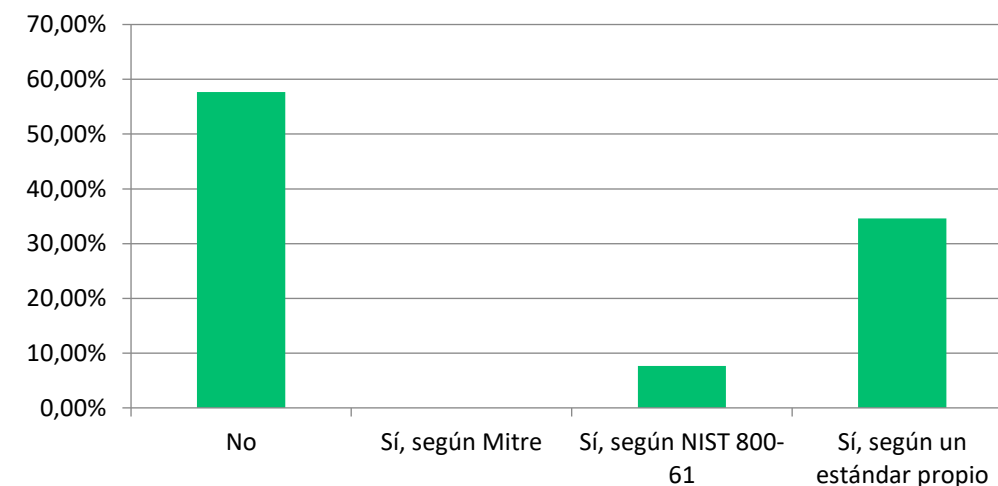
ECOSISTEMA CONSULTADO – PROCEDIMIENTOS

✓ PRIORIZACIÓN

¿Los protocolos incluyen definiciones para establecer la severidad de los ataques y de los activos impactados?



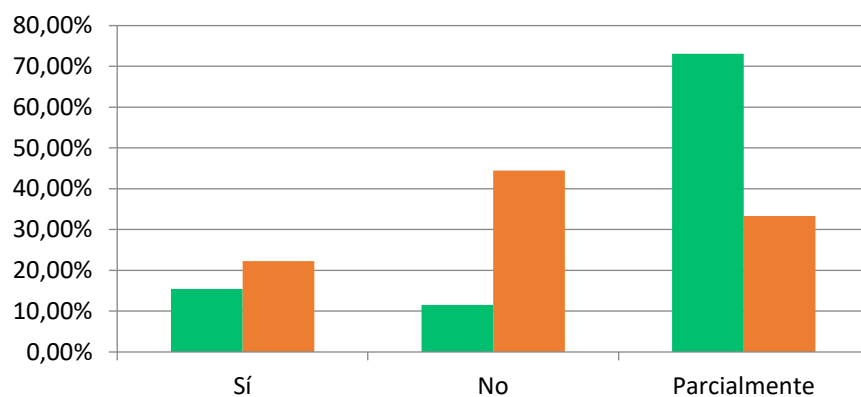
¿Los protocolos incluyen definiciones para establecer la fase del ataque en que se encuentra la planta industrial de acuerdo con algún estándar?



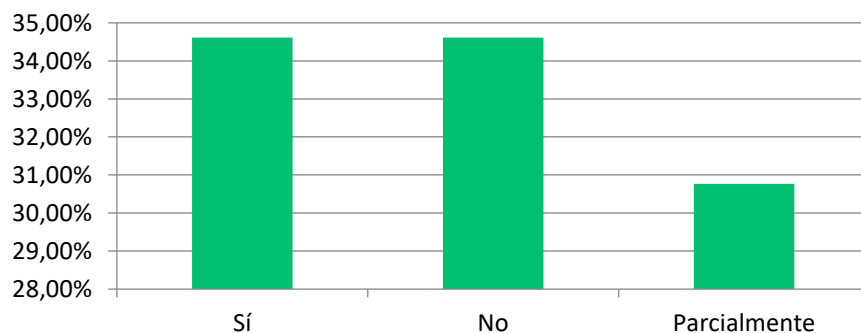
Gestión de Grandes Incidentes

ECOSISTEMA CONSULTADO – FORMACIÓN

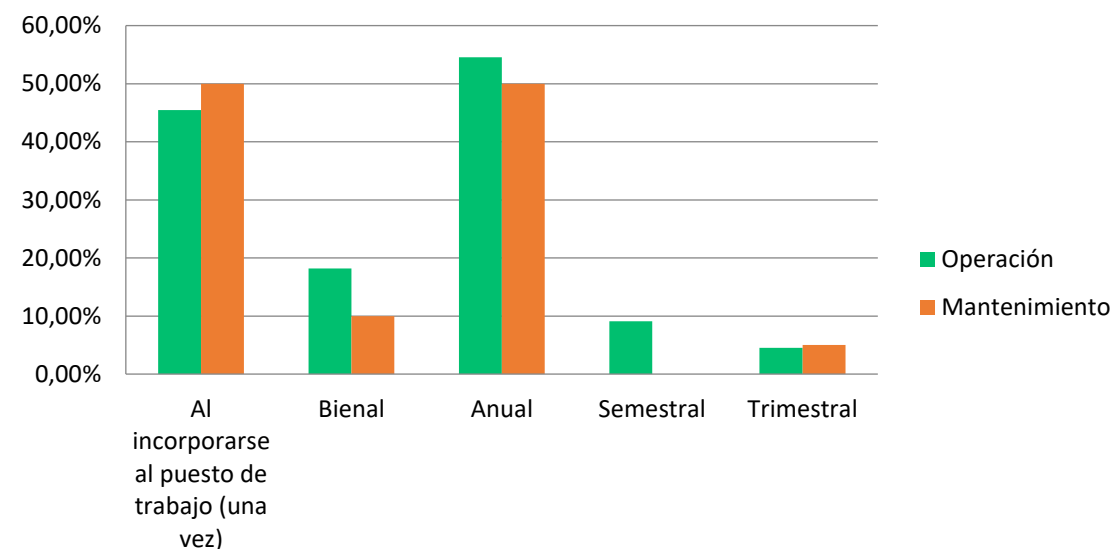
¿Las áreas han sido formadas para identificar comportamientos anómalos relacionados con ciberseguridad?



¿El área de Ciberseguridad está formada para coordinar sus acciones con O&M y prever el impacto en planta de las mismas?



¿Con qué frecuencia las áreas son formadas para identificar comportamientos anómalos relacionados con la ciberseguridad?



✓ FORMACIÓN

Formación



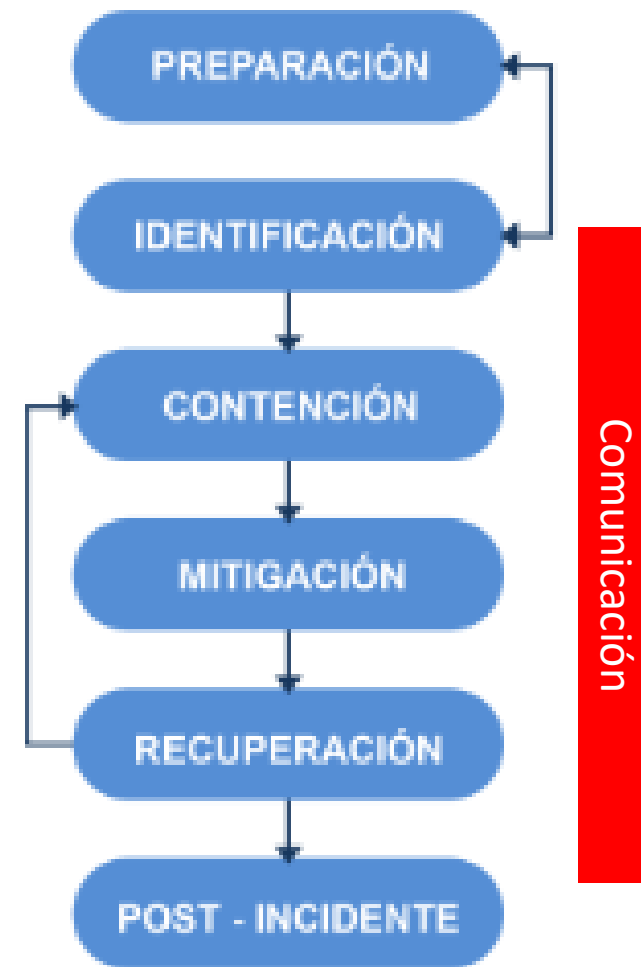
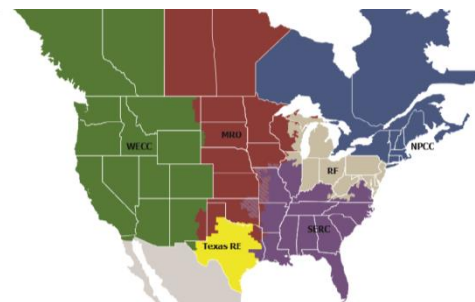
Gestión de Grandes Incidentes

Simulacros

- ✓ Simulacros específicos de ciberseguridad
- ✓ Simulacros interdepartamentales en empresas
- ✓ Simulacros sectoriales / nacionales



GridEx V
GRID SECURITY EXERCISE



Gestión de Grandes Incidentes



Objective 1: Exercise Crisis Response and Recovery

Objective 2: Expand Local and Regional Response

Objective 3: Engage Critical Interdependencies

16 natural gas utilities, 13 water utilities, 3 telecom companies, 277 electric entities (56 natural gas)

Objective 4: Increase Supply Chain Participation

Objective 5: Improve Communication

internal communications response plans.

external communications response plans with other electricity industry entities.

external communications response plans with other non-electricity industry org.

external communications response plans with other critical infrastructure sectors.

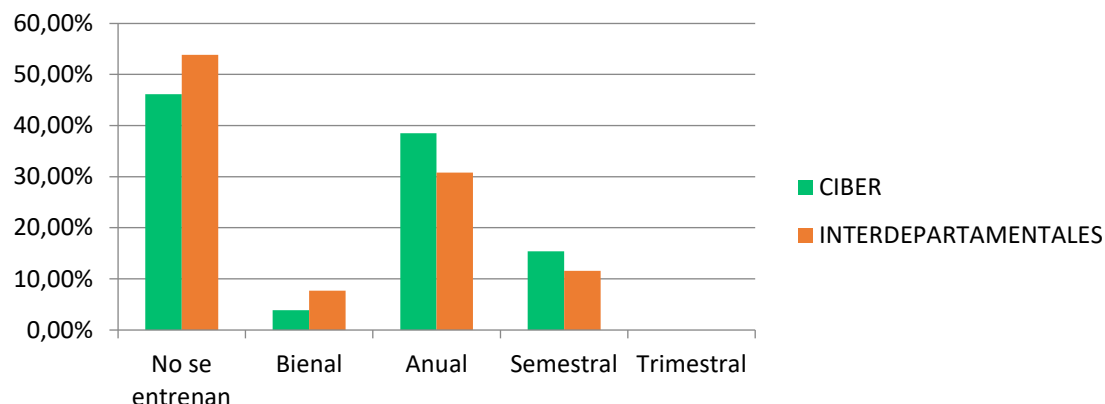
Objective 6: Identify Lessons Learned

Objective 7: Engage Senior Leadership

Gestión de Grandes Incidentes

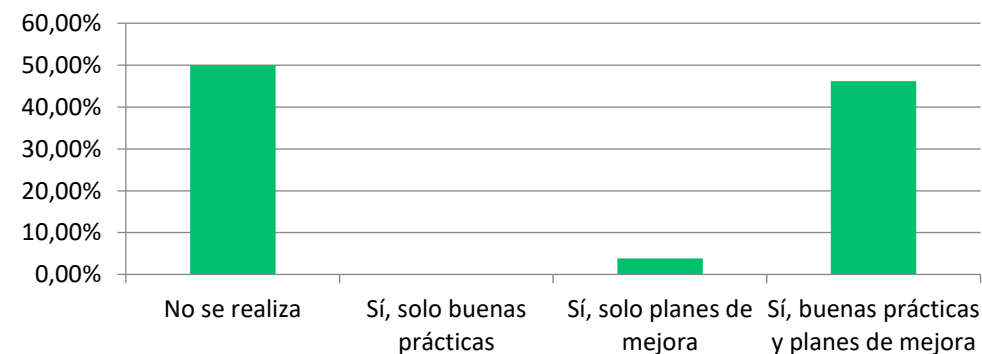
ECOSISTEMA CONSULTADO – SIMULACROS

¿Con qué frecuencia se entrenan ejercicios de incidentes de ciberseguridad por los equipos de ciberseguridad?



✓ Lecciones Aprendidas

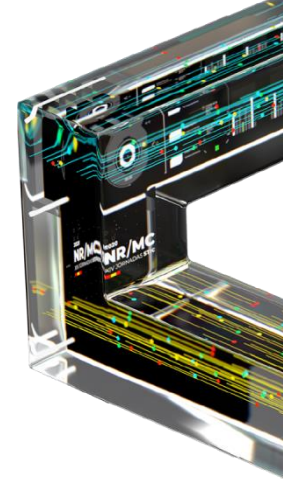
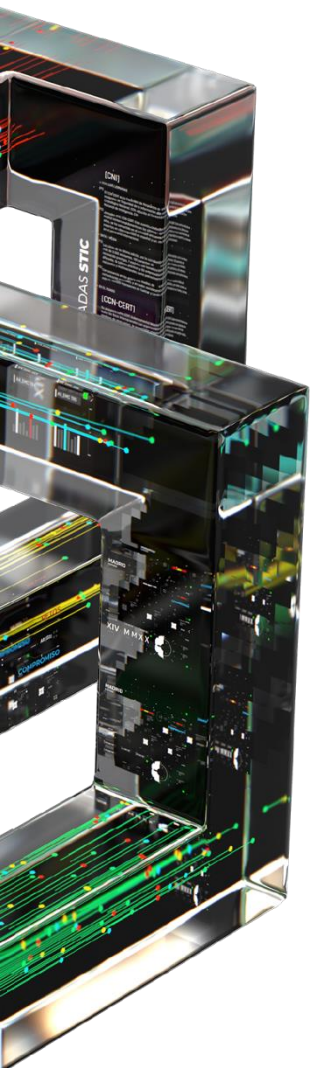
¿Se identifican buenas prácticas y se establecen planes de acción de mejora después de la realización de un ejercicio de incidentes de ciberseguridad?



Gestión de Grandes Incidentes

Conclusiones

- ✓ No hay receta única
 - ✓ Distintas organizaciones → Orientación a riesgos
- ✓ La ciberseguridad debe integrarse en la Gestión de Emergencias
- ✓ Más formación a nivel industrial → Herramientas 
- ✓ Simulacros que integren la parte ciber + O&M
 - ✓ Lecciones aprendidas
- ✓ Seguir avanzando en simulacros sectoriales
- ✓ Reforzar Comunicaciones y Liderazgo



MUCHAS GRACIAS

#XIVJORNADASCCNCERT