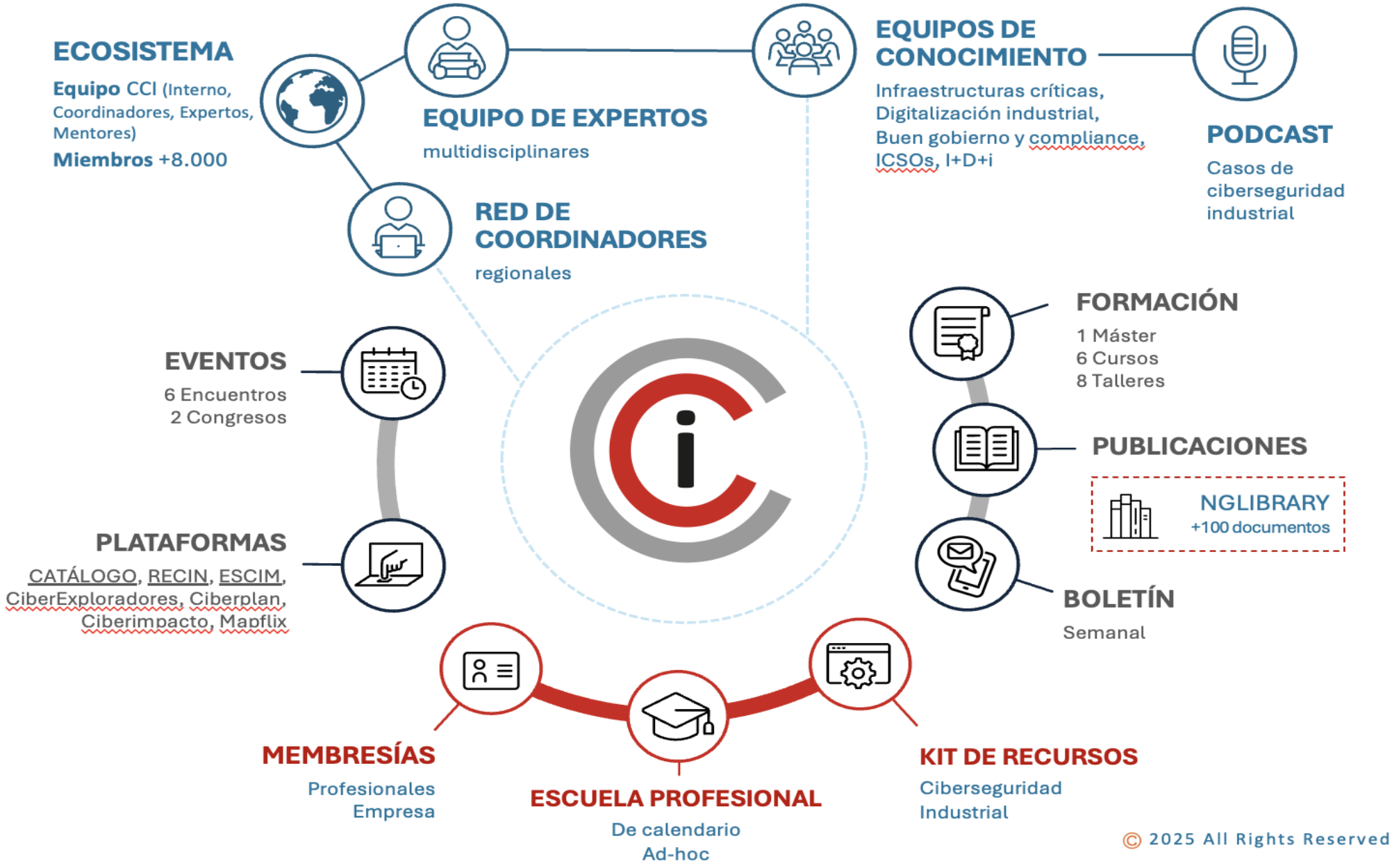
CIBERSEGURIDAD ANTE ESCENARIOS DE ALTO IMPACTO POR PROTECCIONES ELECTRICAS

cigre Colombia



CIGRE (**C**onsejo **I**nternacional de **Gr**andes Sistemas **E**léctricos)

Fundado en **1921**, con miembros en 80 países

Objetivos

- Desarrollar y facilitar el intercambio de conocimiento e información de ingeniería en el campo de los sistemas eléctricos
- Agregar valor al conocimiento e información intercambiada al sintetizar las practicas del estado del arte y el mundo
- Poner el trabajo de CIGRE al servicio de la industria elecrica
- Promover la investigación relevante para los sistemas de energía electrica

El desarrollo, operación y administración de los sistemas de energía así como su diseño, construcción y mantenimiento, son el núcleo de la misión de CIGRE

Como **premisas básicas**, sabemos que los sistemas eléctricos son

- De consumo en tiempo real
- Pequeñas variaciones de frecuencia puede provocar fallas
- Los centros de control deben actuar en milisegundos para mantener la red en parámetros operativos
- Si las protecciones (IED intelligent Electronic Devices) fallan podríamos tener daños en equipos muy caros y difíciles de reemplazar

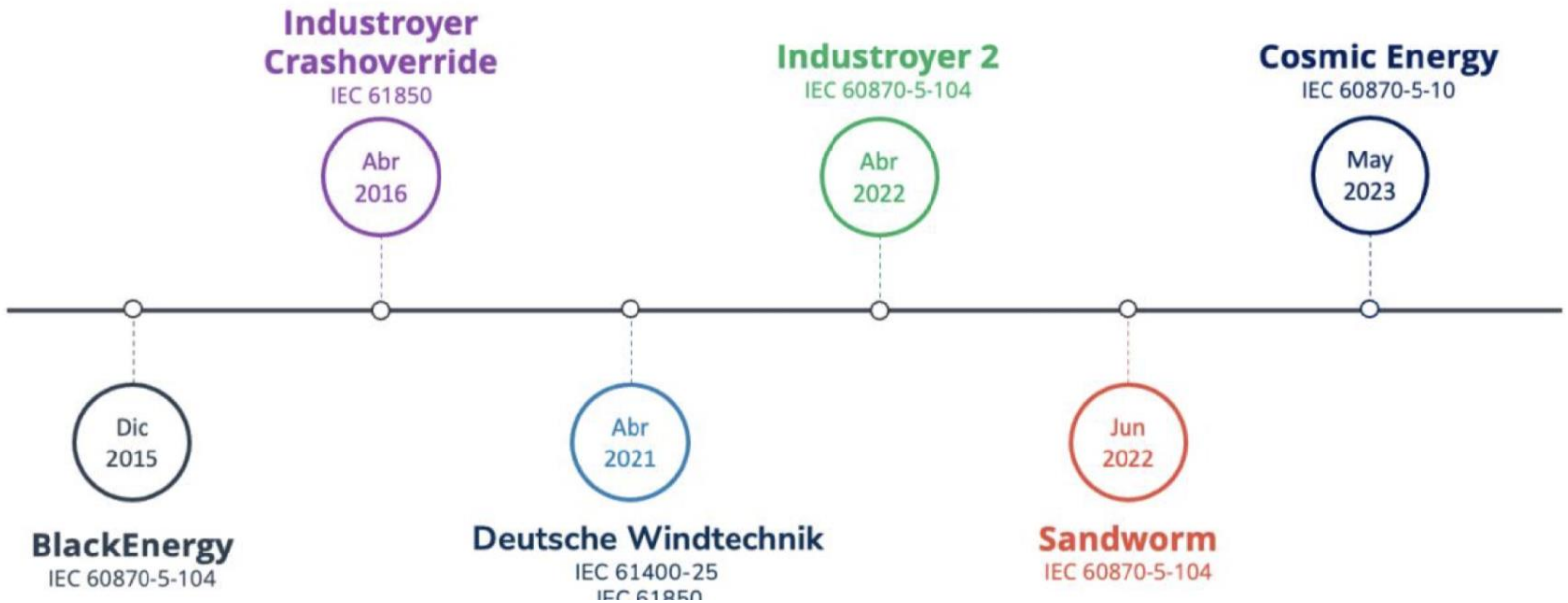
Consideremos que existen casos provocados por un ataque y otros por fallas

- Por ejemplo en el 2015 ucrania tuvo un ciberataque que dejo 225 mil usuarios
- En chile en 2025 fue una falla en una nueva también el apagón de abril 2025 en España develo la fragilidad y la dependencia de la energía eléctrica en el funcionamiento de la sociedad.
- Contar un poco lo que paso.(afecto transporte hospitales, redes, Servicios básicos)

cigre Colombia

Los que fueron ataques al sector eléctrico mas conocidos afectaron e ingresaron por distintas partes

Afectaron distintos dispositivos - áreas



Black energy Ucrania 2015

Comprometió: las protecciones

Afecto: varias subestaciones

Tiempo 6 horas.

230000 usuarios

Ingreso por: Accesos remotos a Scada

Deutsche Windtechnik 2021

Comprometió: la generación de energía eólica

Tiempo **2** días.

No se informó que protocolo afecto, sin embargo se cree que fue ransomware

Industroyer 2022

Comprometió: comunicación entre los sistemas de automatización de las subestaciones y los centros de control

Afecto: modifico el comportamiento de los IED y desactivó protecciones

Tiempo 6 horas.

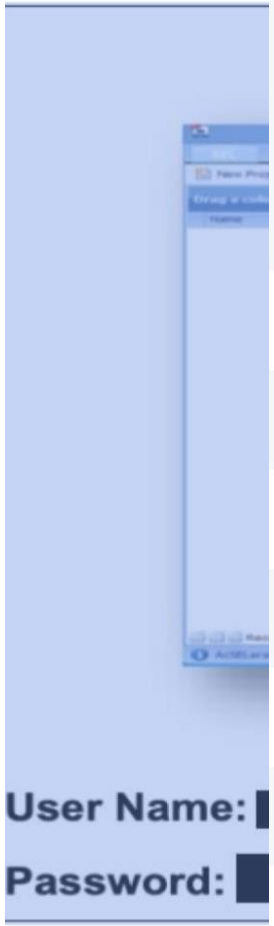
Ingreso por: fue una nueva variante del malware industroyer

Anteriormente los sistemas que gestionan las redes eléctricas estaban aislados y tenían la ventaja de no preocuparse por la ciberseguridad sino si debian preocuparse por el SAFETY

cigre Colombia

Las contraseñas más comunes

Ranking de las contraseñas más utilizadas en 2024*



		Número de veces que se usó	Tiempo para descifrarla (en segundos)
1.	**123456**	3.018.050	**<1**
2.	**123456789**	1.625.135	**<1**
3.	**12345678**	884.740	**<1**
4.	**password**	692.151	**<1**
5.	**qwerty123**	642.638	**<1**
6.	**qwerty1**	583.630	**<1**
7.	**111111**	459.730	**<1**
8.	**12345**	395.573	**<1**

* De acuerdo con un análisis de una base de datos de 2,5TB procedente de 44 países.

Fuente: NordPass

cigre Colombia

SHODAN
Computer Search Engine

SHODAN es el buscador de Infraestructuras

cigre Colombia

SHODAN | Explore | Downloads | Pricing | mar del plata

TOTAL RESULTS

11

TOP PORTS

1701	6
161	4
8083	1

TOP ORGANIZATIONS

Telefonica de Argentina	5
Telecom Personal Bs As	2
AMX Argentina S.A.	1
InterBS S.R.L. (BAEHOST)	1
Interredes S.A.	1

More...

TOP PRODUCTS

MikroTik	3
Apache httpd	1
net-snmp	1

View Report | View on Map | Advanced Search

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

186.127.243.2
host2.186-127-243.telecom.net.ar
Telecom Personal Bs As
Argentina, Mar del Plata

```
SNMP:
  Uptime: 250654330
  Description: Linux haivision-ace 2.6.37 #1 PREEMPT Mon Aug 14 18:28:19 EDT 2017 armv7l
  Service: 72
  Versions:
    1
    3
  Name: haivision-ace
  Ordescr: The MIB module for SNMPv2 entities
  Engineid Format: mac
  Contact: AE-Video <ae-vid@cablevisionfibertel.mail....
```

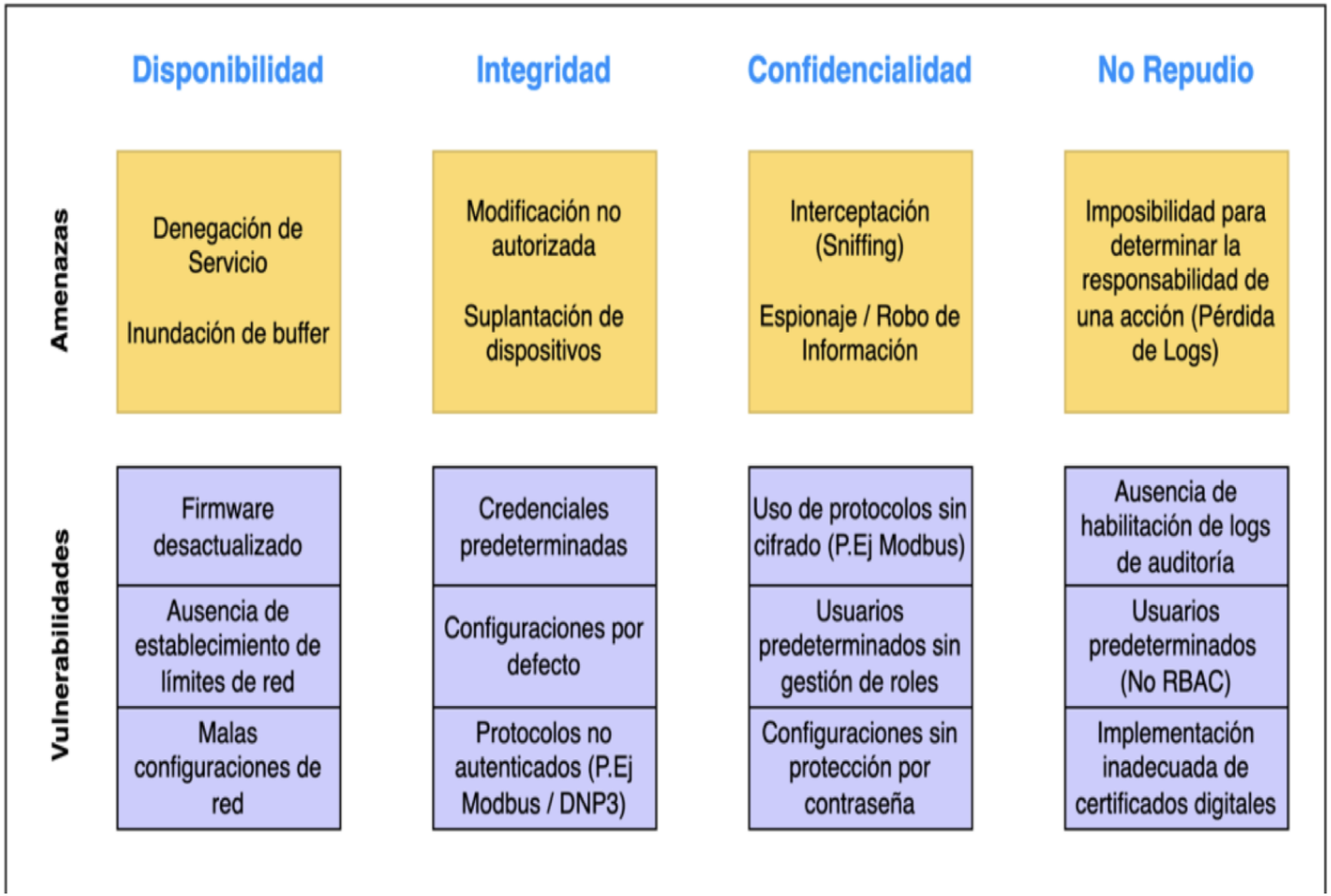
200.5.229.60
Telefonica de Argentina
Argentina, Buenos Aires

```
\xc8\x02\x00n\x00\x00\x00\x00\x00\x00\x00\x01\x80\x08\x00\x00\x00\x00\x00\x02\x80\x08\x00\x00\
```

181.84.105.40
host40.181-84-105.telecom.net.ar
Telecom Personal Bs As
Argentina, Mar del Plata

```
SNMP:
  Uptime: 36039400
  Description: RouterOS RB750r2
  Service: 78
  Versions:
    1
```

Este método aprovecha operadores de búsqueda especializados como site:, filetype:, intitle:, inurl:, intext: y cache: para refinar las consultas y buscar contenido específico como archivos ocultos, documentos confidenciales, bases de datos expuestas o vulnerabilidades de seguridad.


Disponibilidad
Integridad
Confidencialidad
No Repudio
Amenazas
Denegación de Servicio
Inundación de buffer
Modificación no autorizada
Suplantación de dispositivos
Interceptación (Sniffing)
Espionaje / Robo de Información
Imposibilidad para determinar la responsabilidad de una acción (Pérdida de Logs)
Vulnerabilidades
Firmware desactualizado
Ausencia de establecimiento de límites de red
Malas configuraciones de red
Credenciales predeterminadas
Configuraciones por defecto
Protocolos no autenticados (P.Ej Modbus / DNP3)
Uso de protocolos sin cifrado (P.Ej Modbus)
Usuarios predeterminados sin gestión de roles
Configuraciones sin protección por contraseña
Ausencia de habilitación de logs de auditoría
Usuarios predeterminados (No RBAC)
Implementación inadecuada de certificados digitales

Engaños

cigre Colombia

El engaño Ingeniería Social es lo que se utiliza para obtener información

Y esto no es de ahora **Vendieron la tour Eiffel 2 veces**

Victor Lustig, el hombre que vendió la torre Eiffel dos veces

• Timó a Al Capone, patentó una máquina de copiar dinero y llegó a vender la torre Eiffel... dos veces. Por esas y otras argucias, Victor Lustig se ha ganado el sobrenombre del mayor estafador del siglo XX

En 1925 los franceses querían deshacerse de la Tour Eiffel porque decían que era fea y querían desarmarla y vender la chatarra
Este señor se enteró y decidió decir que el era el que tramitaba esa venta y allí empezó el engaño
Les dejo el link del articulo para que lean toda la historia

https://www.lavanguardia.com/historiayvida/historia-contemporanea/20210425/6989398/victor-lustig-hombre-vendio-torre-eiffel.html

cigre
Colombia

NORMATIVA para un DISEÑO SEGURO

North American Electric Reliaility Corporation Critical Infrastructure Protection

Requisitos de planificación y operación del sistema de Energía de América del Nort

The ISA/IEC 62443 series of standards

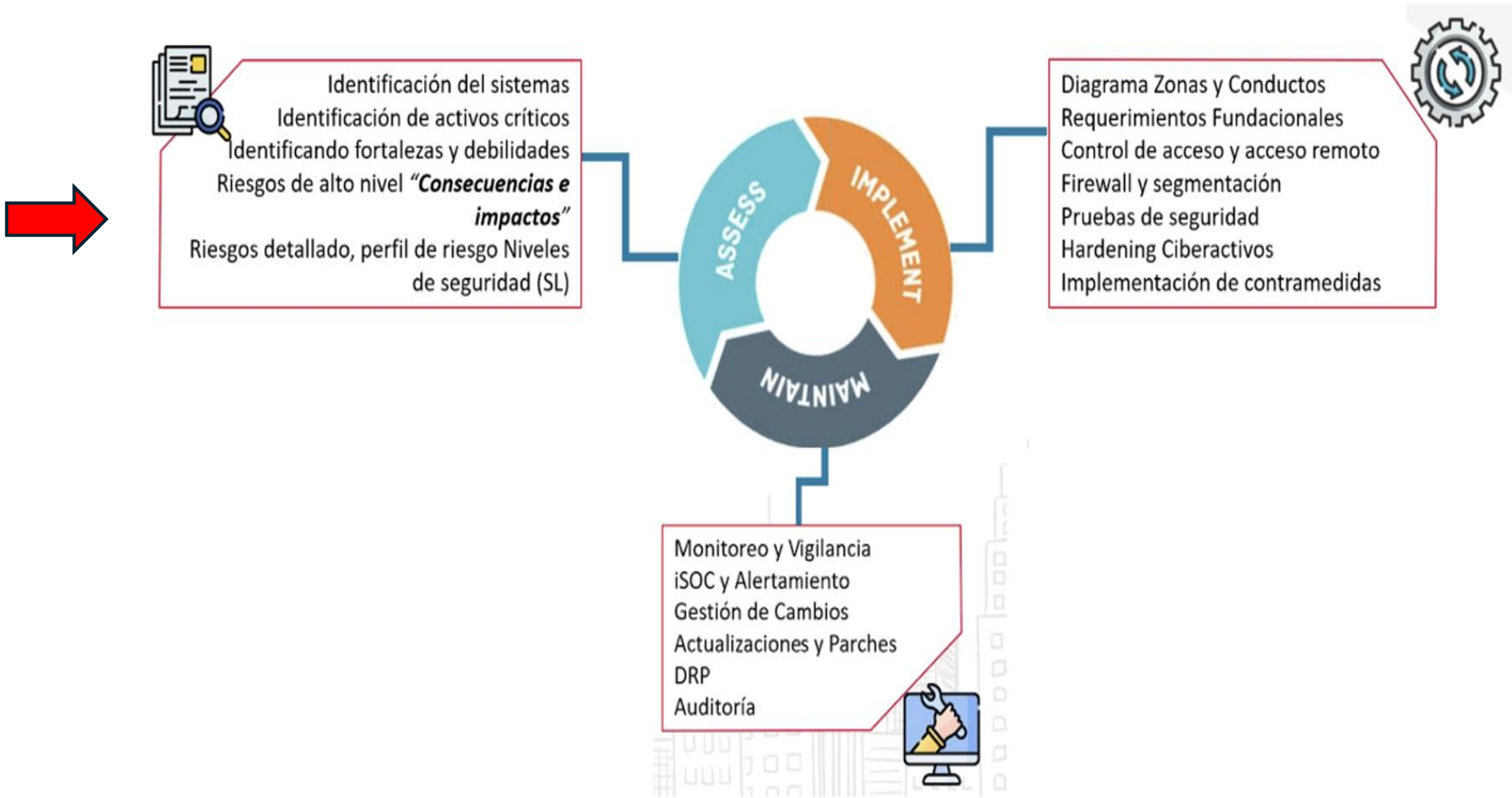
Aborda el tema de ciberseguridad para sistemas de automatización y control industrial (IACS) cubriendo aspectos para la gestión de ciberseguridad industrial, desarrollo seguro de productos, requisitos para componente y gestión de riesgos

ISO 27019

Enfoca los controles de seguridad de la información de la ISO27002:2013 a los sistemas de control y tecnologías de automatización, , permitiendo gestionar la seguridad de sistemas utilizados por las empresas del sector eléctrico, como generación , transmisión, y distribución.

PRIMERA MEDIDA: INVENTARIO

Estándar ISA/IEC 62443



PRIMERA MEDIDA: INVENTARIO

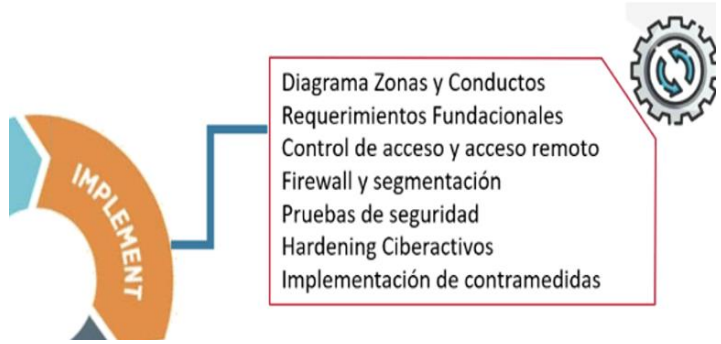
PRIMERA MEDIDA: INVENTARIO

NIST National Institute of Standards and Technology
Center of Excellence

NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	**CSF 2.0 Category**	**CSF 2.0 Category Identifier**
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	[illegible]	[illegible]
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
	[illegible]	[illegible]
Protect (PR)	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

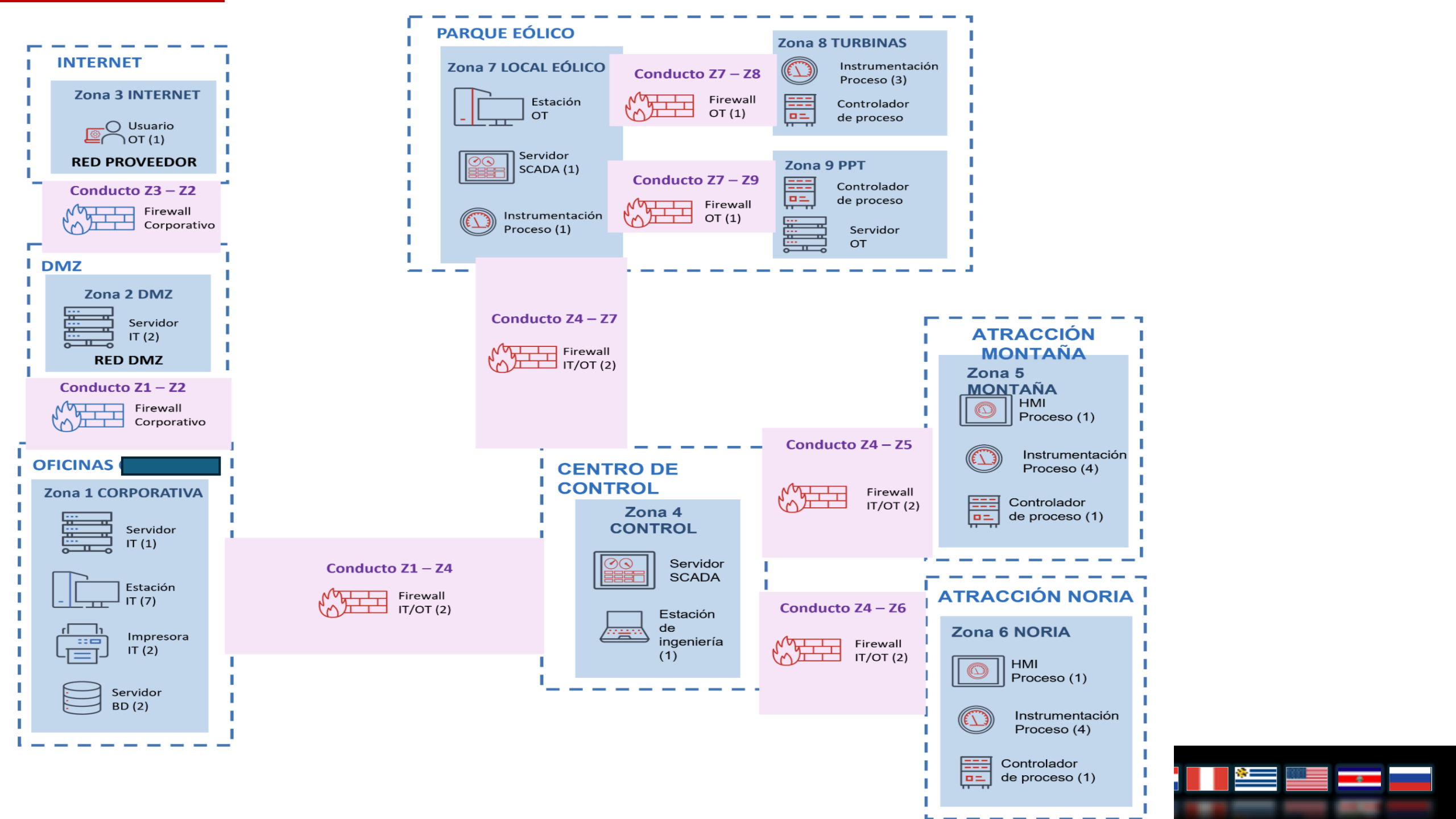
cigre Colombia

DEFINIR ZONAS Y CONDUCTOS



RECIN es una plataforma online diseñada para ayudar a las empresas a evaluar de manera rápida y sencilla el nivel de ciberseguridad en sus proyectos industriales desde el diseño. Se pueden incluir la ***información de zonas y conductos*** y los componentes para cada caso, e inmediatamente se visualiza armado un mapa que cumple con el estándar

Esta herramienta eficaz y segura que permite además clasificar los niveles de criticidad en disponibilidad, integridad y confidencialidad a cada zona, conducto y componente que reflejan en el gráfico permitiendo identificar potenciales riesgos. Al utilizar **RECIN**, se puede obtener un informe del proyecto de forma ágil, con todos los requisitos de ciberseguridad establecidos en la norma ISA/IEC 62443-3-3, pudiéndolo visualizar ya sea por vista de zonas y conductos, o por vista de requisitos fundamentales.


INTERNET
Zona 3 INTERNET
Usuario OT (1)
RED PROVEEDOR
Conducto Z3 – Z2
Firewall Corporativo
DMZ
Zona 2 DMZ
Servidor IT (2)
RED DMZ
Conducto Z1 – Z2
Firewall Corporativo
OFICINAS
Zona 1 CORPORATIVA
Servidor IT (1)
Estación IT (7)
Impresora IT (2)
Servidor BD (2)
Conducto Z1 – Z4
Firewall IT/OT (2)
PARQUE EÓLICO
Zona 7 LOCAL EÓLICO
Estación OT
Servidor SCADA (1)
Instrumentación Proceso (1)
Conducto Z7 – Z8
Firewall OT (1)
Zona 8 TURBINAS
Instrumentación Proceso (3)
Controlador de proceso
Conducto Z7 – Z9
Firewall OT (1)
Zona 9 PPT
Controlador de proceso
Servidor OT
Conducto Z4 – Z7
Firewall IT/OT (2)
CENTRO DE CONTROL
Zona 4 CONTROL
Servidor SCADA
Estación de ingeniería (1)
Conducto Z4 – Z5
Firewall IT/OT (2)
Conducto Z4 – Z6
Firewall IT/OT (2)
ATRACCIÓN MONTAÑA
Zona 5 MONTAÑA
HMI Proceso (1)
Instrumentación Proceso (4)
Controlador de proceso (1)
ATRACCIÓN NORIA
Zona 6 NORIA
HMI Proceso (1)
Instrumentación Proceso (4)
Controlador de proceso (1)

Definir roles y responsabilidades de cada actor dentro los sistemas incluyendo internos y externos especialmente la cadena de suministro (proveedores)
ICSO Industrial Chief Security Officer

Realizar un análisis de riesgo basado en una metodología probada y enfocada a los entornos industriales (IEC 62443-3-2 y ESCIM)

Diseno de arquitecturas seguras usando zonas y conductos
Control 8.22 de las ISO27019 y sección 8 de la IEC 62443-2-1

Políticas y soluciones de Acceso remoto - MFA

cigre Colombia

Ciber-ejercicios para revisar los controles

ESCIM

ESCIM es una plataforma online diseñada para desarrollar ejercicios de simulación de escritorio (TableTop Exercise) en el ámbito de la ciberseguridad industrial, ayudando a las organizaciones a modelar y presentar escenarios de ciberincidentes de alto impacto.

Su finalidad es la realización de ciberejercicios que permitan revisar los controles de ciberseguridad, evaluar la eficacia de los procesos y procedimientos existentes, y poner a prueba la coordinación y comunicación entre las distintas áreas de la organización. Con ello, **ESCIM** contribuye a anticiparse y prepararse frente a los ciberincidentes que afecten a los entornos OT.

La plataforma permite analizar distintos tipos de incidentes que podrían afectar a un sector o proceso automatizado específico, gracias a su integración con las matrices MITRE ATT&CK, tanto en su versión Enterprise como ICS. Además proporciona un marco estructurado para estudiar las fases de preparación, identificación, contención y recuperación de incidentes, alineado con el ciclo de vida de un incidente definido por el framework de NIST.

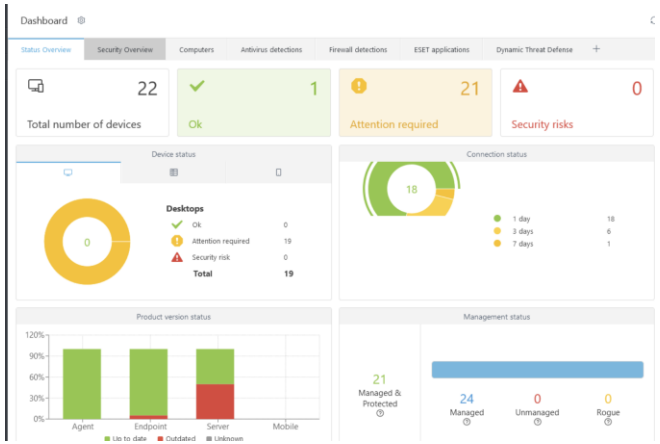
Definir Políticas y procedimientos (revisarlos periódicamente y cuando haya actualizaciones - definir responsable)

Definir un standard de configuraciones y mantenerlas en respaldo

Control de Acceso, pero que no sea fácil de descifrar
Definir reglas de contraseñas fuertes

Y probar su restauración

Capacitación



Logs

Control de acceso
Basado en Roles

MACIN

Modelo de evaluación de madurez

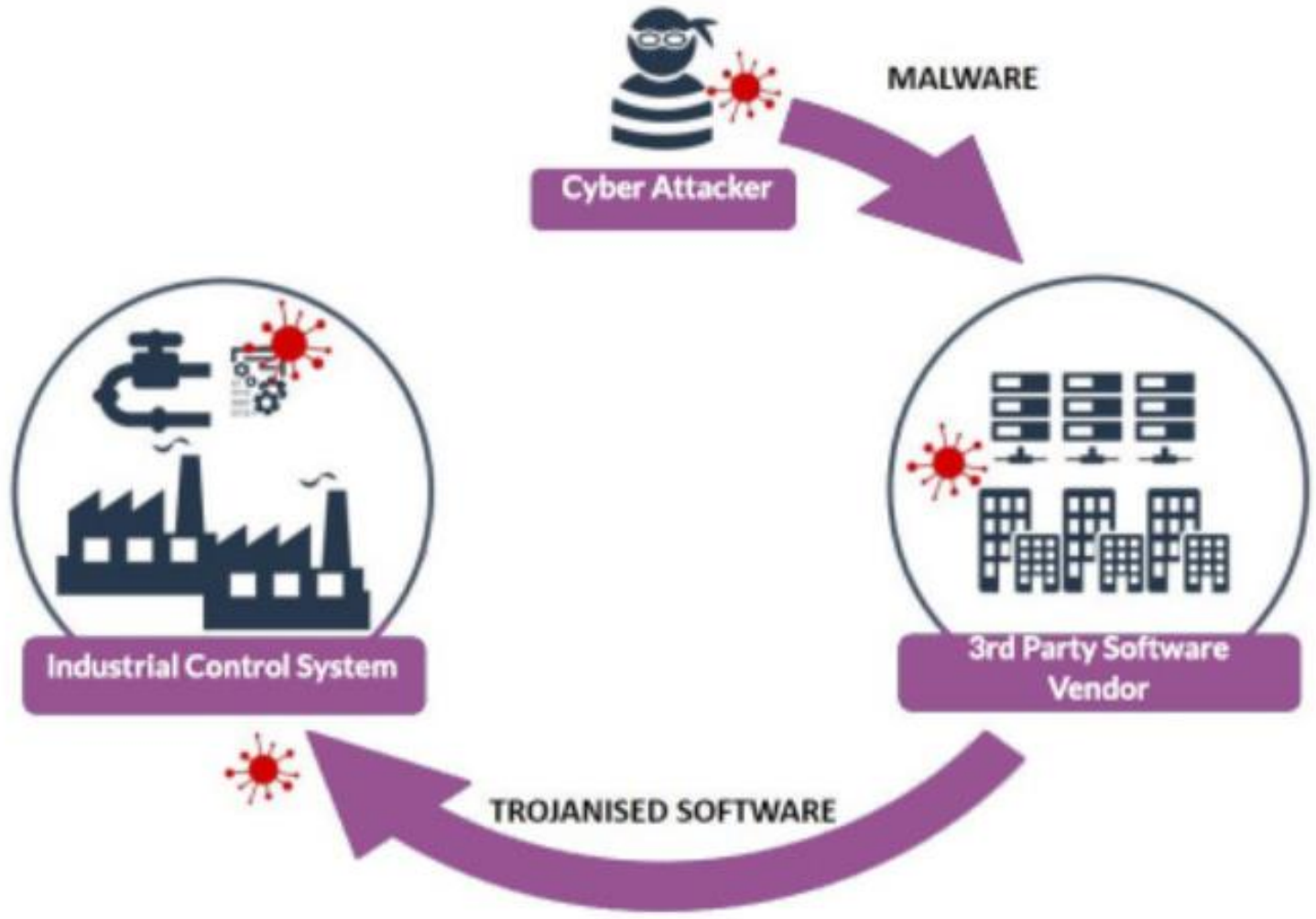
175 PRÁCTICAS AGRUPADAS EN 45 OBJETIVOS DE 10 DOMINIOS

INICIADO · DEFINIDO · REPETIBLE · GESTIONADO · OPTIMIZADO

	ESTRATEGIA, GOBERNANZA y CUMPLIMIENTO DE CIBERSEGURIDAD (EGCC)	GESTIÓN DE ACTIVOS (GA)	GESTIÓN DE AMENAZAS Y VULNERABILIDADES (GAV)	GESTIÓN DE RIESGOS (GR)	GESTIÓN DE IDENTIDADES Y ACCESO (GIA)	ARQUITECTURA (A)	GESTIÓN DE LA CADENA DE SUMINISTRO Y TERCEROS (GCST)	GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD (GIC)	RESILIENCIA OPERATIVA (RO)	GESTIÓN DEL PERSONAL (GP)
Procesos	22	17	18	15	17	20	21	18	17	10
Personas	22	17	18	15	17	20	21	18	17	10
Tecnologias	22	17	18	15	17	20	21	18	17	10
Resultados	22	17	18	15	17	20	21	18	17	10

Es una cámara profesional de formato completo, con objetivos intercambiables y medición por capas, diseñada para capturar detalle técnico y contexto organizativo con precisión.

Ciber-riesgos en la cadena de suministros



cigre Colombia

JLR Cyber Incident Marks Latest Blow in UK's Cyber Crime Wave

Date: 4 September 2025

cigre Colombia

1. *Cierre total de la producción en cinco plantas* importantes, incluidas las de Halewood, Solihull y Wolverhampton.

2. Los *concesionarios no pueden registrar vehículos*, *acceder a piezas ni realizar el mantenimiento de los automóviles.*

3. Se ha *confirmado la filtración de datos* (aún no se han revelado los detalles). Se estima que **JLR ha perdido 50 millones de libras esterlinas** hasta ahora. (25/sept)

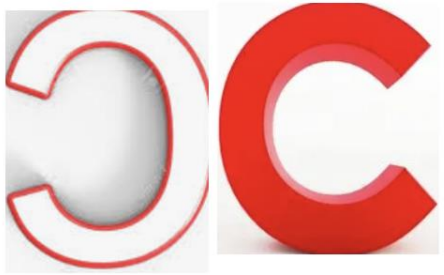
4. Se espera que el *mayor impacto recaiga sobre los proveedores pequeños* y medianos; los expertos afirman que *muchos podrían declararse en quiebra*.

5. El Gobierno del *Reino Unido se enfrenta a peticiones* para que se apruebe un plan de permisos para evitar una *pérdida generalizada de puestos de trabajo*.

6. Más de tres semanas de interrupción del servicio en la actualidad. (25/Sept)

CULTURA

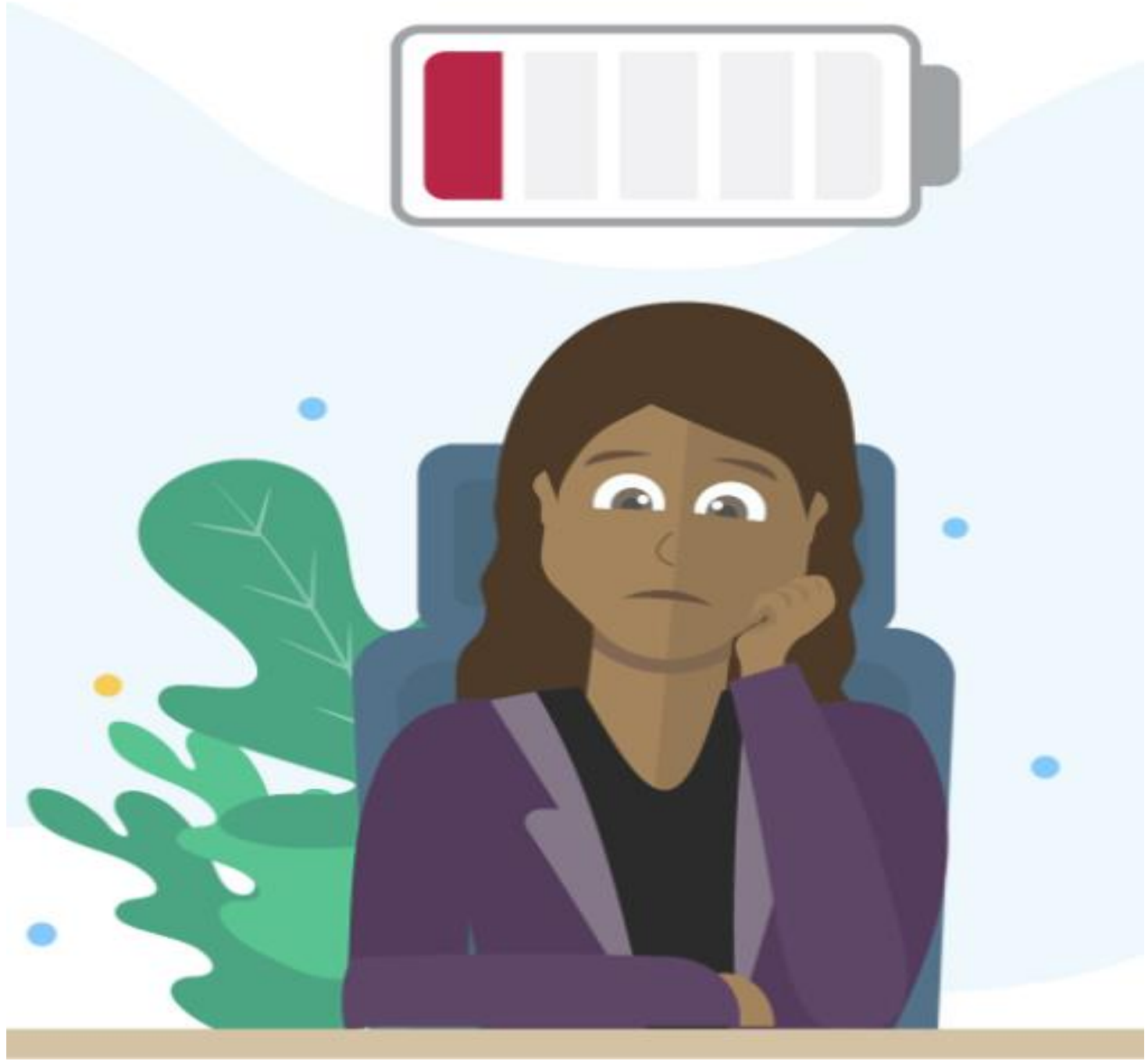
COMPARTIR



COLABORAR

CIBERSEGURIDAD

cigre Colombia



MUCHAS GRACIAS!!

- NORA SUSANA ALZUA
- NORA.ALZUA@AR.CCI-ES.ORG
- @ALZUANORA
- HTTPS://WWW.LINKEDIN.COM/IN/NORA-ALZUA/

Cadena de Suministro: El riesgo es no conocer sus riesgos

cigre Colombia