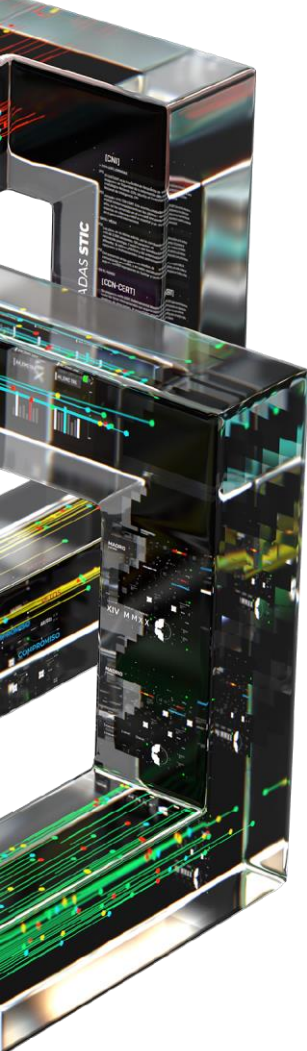




#XIVJORNADASCCNCERT

**“EMMA-ANA, afianzando el
ecosistema CCN-CERT con
integraciones de valor añadido”**



**Alejandro
Martín**

**Sidertia
Solutions S.L**

**Dirección
Técnica**

amartin@sidertia.com



#XIVJORNADASCCNCERT



**Darragh
Kelly**

**Open Cloud
Factory**

**Director de
Go-to-Market y
Alianzas
estratégicas**

darragh.kelly@opencloudfactory.com



1. EMMA: Vigilancia sobre la red

- **EMMA-** Vigilancia sobre la red
 - Visibilidad de la superficie de exposición
 - CMDB
 - **EMMA – Cumplimiento (ROCIO)**
 - Vigilancia de las deficiencias en las configuraciones de la electrónica de la red
 - Facilitar partes de la auditoría de las configuraciones de manera centralizada y automatizada

Dashboard		Network Devices					
☐	IP	IP Management	Backup connection type	Brand/Model	Compliance status	Tags	i
☐	10.10.37.5		SSH	Cisco/Generic	0 0 ★	None	
☐	10.240.5.10			Cisco/Generic		1	
☒	10.10.36.45		SSH	Cisco/Generic	100 0 ★	16 21	
IP: 10.10.36.45 IP Management: Description: Serial number: FOC1809W0TU CPE: SNMP version: SNMP RW: SNMP v3 Security level: SNMP v3 Authorization pass phrase: ***** SNMP v3 Privacy pass phrase: ***** CoA port: Purchase date: Warranty: EOL: User: Privilege user: IP Management: Hostname: switch-dc-dev Version: 15.0(2)SE5 MAC Address: 28:34:A2:8C:88:80 SNMP RO: SNMP v3 Security name: SNMP v3 Authorization protocol: SNMP v3 Privacy protocol: CoA password: ***** Disconnection type: Purchase order: Maintenance: Connection type: Password: ***** Location:							

2. EMMA: Vigilancia de las deficiencias

- *EMMA – Cumplimiento (ROCIO)*
 - Vigilancia de las deficiencias en las configuraciones de la electrónica de la red
 - Facilitar partes de la auditoría de las configuraciones de manera centralizada y automatizada
 - Copias de seguridad

☐	Name	Description	Tag (without prefix)	Type	Vendors	Flags	i
☐	ARUBA_SSH_ENABLED	Check if ssh is enabled	ARUBA_SSH_ENABLED	dynamic	Aruba		
☐	AWPLUS_SSH_ALLOW_USERS_ENABLED	Check if ssh allows at least one user	AWPLUS_SSH_ALLOW_USERS_ENABLED	static	Aruba		
☐	AWPLUS_SSH_ENABLED	Check if ssh is enabled	AWPLUS_SSH_ENABLED	static	Aruba		
☐	AWPLUS_SSH_VERSION_V2ONLY	Check the version of ssh is v2only	AWPLUS_SSH_VERSION	static	Aruba		
☐	EXTREMEXOS_SSH_2_ENABLED	Check if ssh v2 is enabled	EXTREMEXOS_SSH_2_ENABLED	static	Extremenetworks		
☐	EXTREMEXOS_SSH_2_USER_KEY	Check if ssh v2 have user key	EXTREMEXOS_SSH_2_USER_KEY	static	Extremenetworks		
☐	EXTREMEXOS_SSH_2_USER_KEY_ADD	Check if ssh user key user is	EXTREMEXOS_SSH_2_USER_KEY_ADD	static	Extremenetworks		

Rules					Rules Passed					Rules Failed				
175 Total Rules					80 Total Rules Passed					95 Total Rules Failed				
Hostname	Network Device IP	IP Management	Rule Passed	C	Hostname	Network Device IP	IP Management	Rule Passed	C	Hostname	Network Device IP	IP Management	Rule Failed	C
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_TACACS_SERVER	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_LOGGING_TRAP	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_LOGGING_HOST	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_SNMP_SERVER_ENGINE_ID	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_LOGGING_BUFFERED	2	switch-dc-dev	10.10.36.45	0.0.0.0	IOS_LOGGING_TRAP	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_SERVICE_SEQUENCE_NUMBERS	2	switch-dc-dev	10.10.36.45	0.0.0.0	IOS_LOGGING_HOST	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_TACACS_SERVER	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_PRIVILEGE_EXEC_LEVEL	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_STORM_CONTROL	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_PASSWORD_ENCRYPTION	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_ACCI	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_LOGGING_BUFFERED	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_IP_SSH_V2	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_IP_DOMAIN_NAME	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_ENABLE_SECRET	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_CRYPTO_SPKI_TRUSTPOINT	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2	CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV	2

2. ANA: Introducción

Seguridad

Ayuda a identificar y solucionar anomalías de seguridad en organizaciones

Información

Se alimenta de múltiples fuentes de datos

Centralización

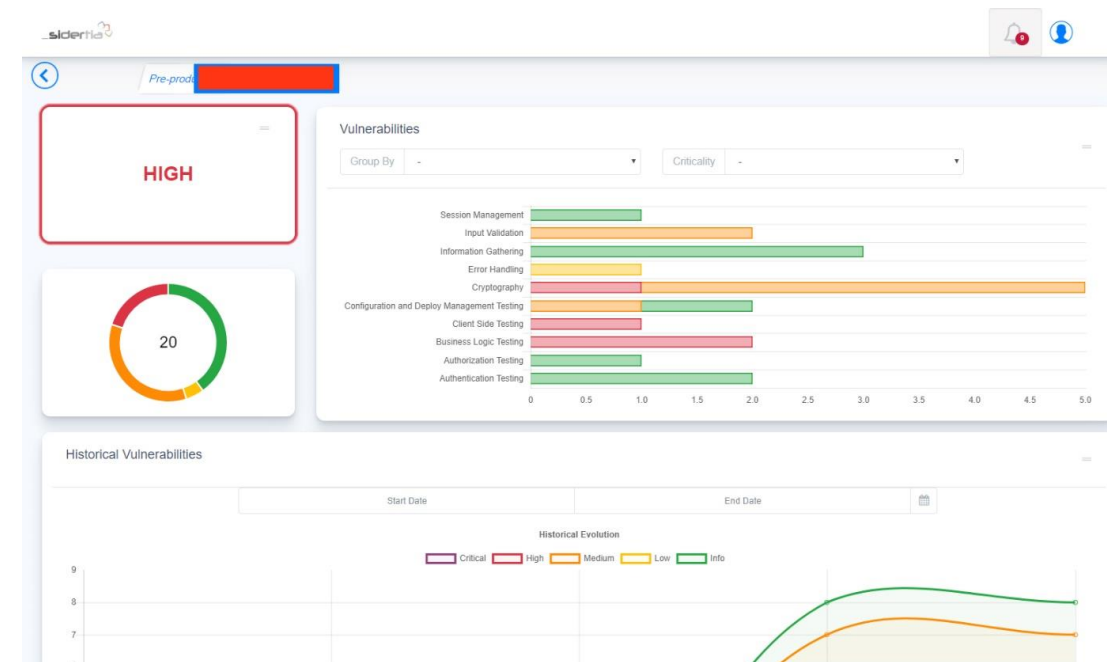
Un único panel de visualización

Integración

Permite trabajar en distintas aplicaciones con un solo esquema de usuarios y Single Sign On

Seguimiento

Para la mejora continua



5. EMMA+ANA

¿Qué podemos hacer?

- Vigilancia en las vulnerabilidades que tienen lugar en los dispositivos de la red
 - Importancia de los CPE's (*Common Platform Enumeration*)
- Consolidación de toda la información
 - Dispositivos
 - Vulnerabilidades
 - Seguimiento de debilidades y cumplimiento



5. EMMA+ANA

Vigilancia de las vulnerabilidades en la electrónica

EMMA

- EMMA recoge y comparte con ANA
 - Resultados de la auditorías de las configuraciones (hallazgos y estadísticas) de los dispositivos de red
 - CPE de dispositivo + contexto



ANA

Enable import ANA reports
☐ Yes

Public key used to import ANA reports
 -----BEGIN PUBLIC KEY-----
 [Redacted Public Key]
 -----END PUBLIC KEY-----
 [Generate new key pair] [Download public key] [Delete key pair]

Enable export ANA reports
☐ Yes

Public key used to export ANA reports
 -----BEGIN PUBLIC KEY-----
 [Redacted Public Key]
 -----END PUBLIC KEY-----
 [Upload public key] [Delete key pair]

8. EMMA+ANA

Consolidación en un mismo sistema

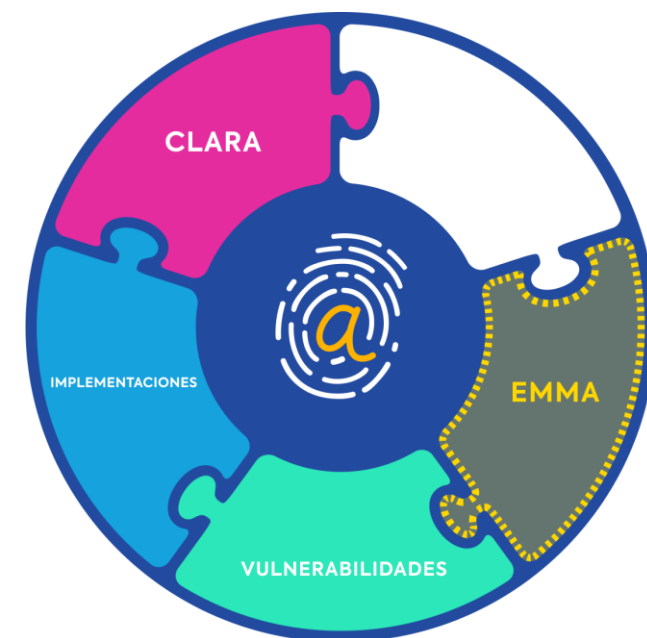
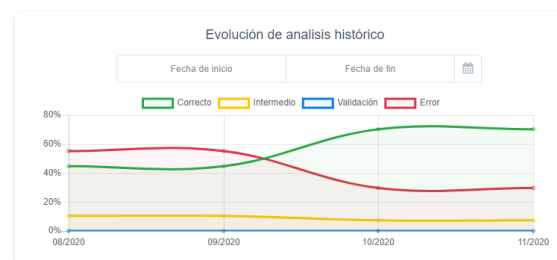
- Visualización centralizada de los dispositivos de red, junto a otros activos de la organización.



- Identificación de vulnerabilidades asociadas a los dispositivos de red.

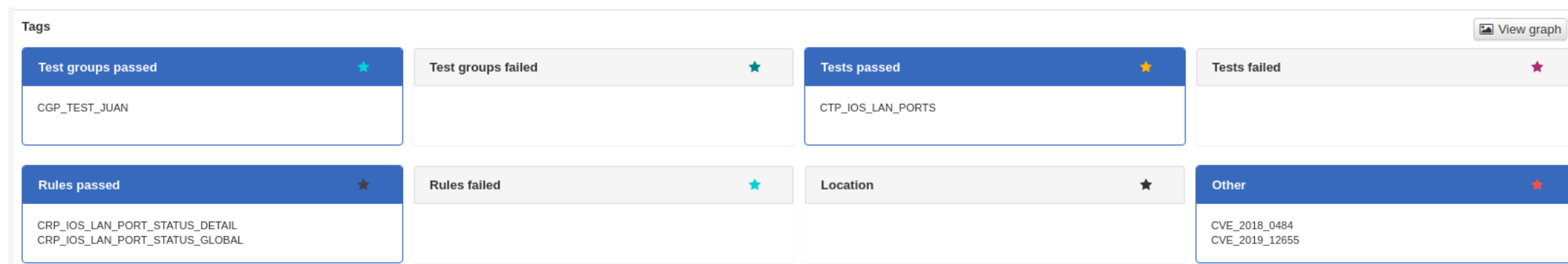


- Seguimiento de los dispositivos de red, tanto de las debilidades como del cumplimiento.



X. EMMA+ANA

Output: Vigilancia de las vulnerabilidades en la electrónica



- Crear cuadro de mando sobre dispositivos por riesgo
- Cuantificar y visualizar dispositivos afectados
- Cuadros de mando para plan de acción (remediación)

x. EMMA+ANA

Resultado global

Rules

175

Total Rules

Rules Passed

80

Total Rules Passed

Rules Failed

95

Total Rules Failed

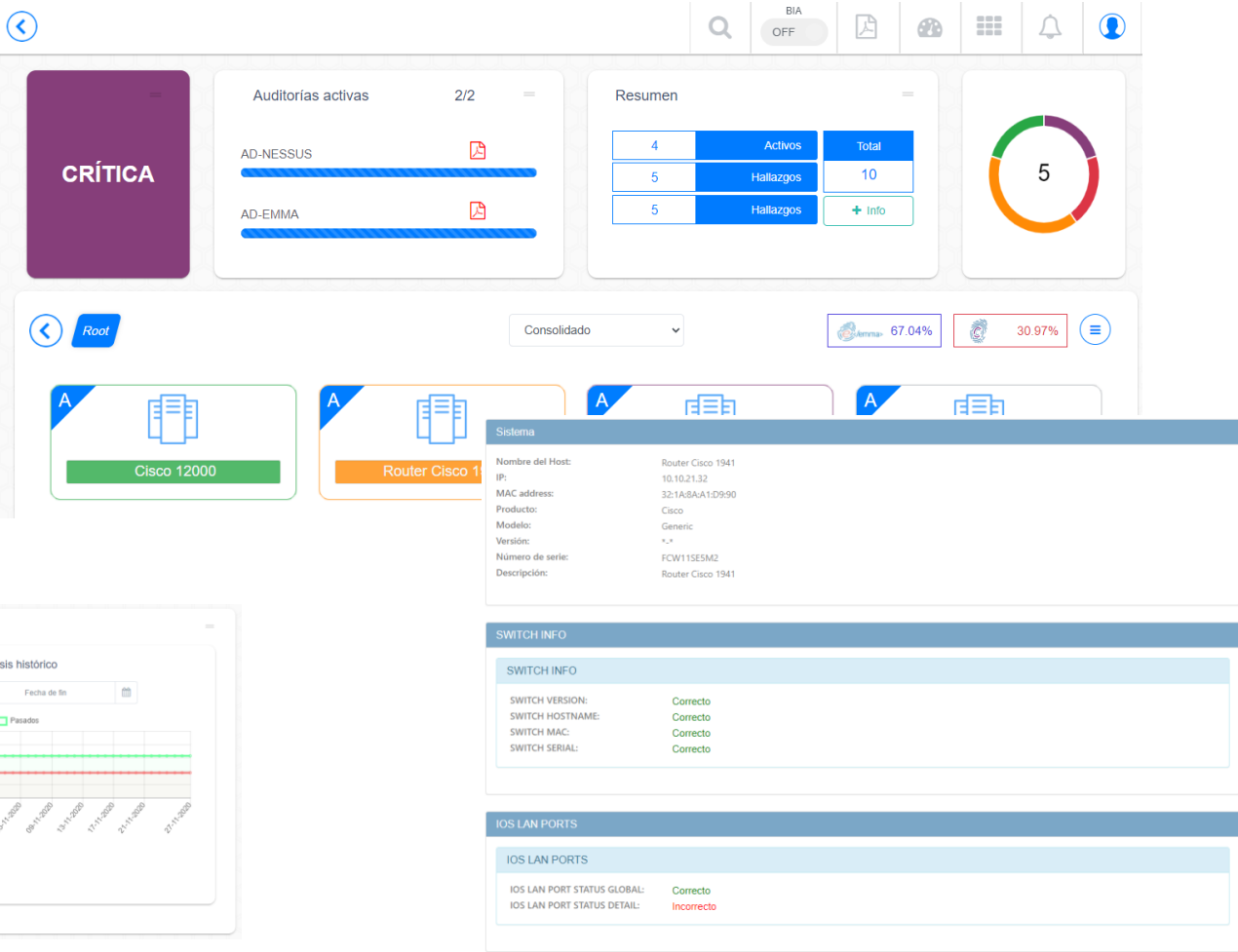
Hostname	Network Device IP	IP Management	Rule Passed	C
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_TACACS_SERVER	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_SNMP_SERVER_ENGINE_ID	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_SERVICE_SEQUENCE_NUMBERS	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_PRIVILEGE_EXEC_LEVEL	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_PASSWORD_ENCRYPTION	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_LOGGING_BUFFERED	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_IP_SSH_V2	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_IP_DOMAIN_NAME	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_ENABLE_SECRET	2
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_CRYPTO_SPKI_TRUSTPOINT	2

Hostname	Network Device IP	IP Management	Rule Failed
CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_LOGGING_TRAP
CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_LOGGING_HOST
CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_LOGGING_BUFFERED
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_LOGGING_TRAP
switch-dc-dev	10.10.36.45	0.0.0.0	IOS_LOGGING_HOST
CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_TACACS_SERVER
CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_STORMCONTROL
CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_PRIV
CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_ACCI
CiscoDemoCenter	10.10.36.49	10.10.36.49	IOS_SNMP_SERVER_USER_V3_VIC

Export: Row

Formatted

1 2 3 4 5 ... 1



X. EMMA+ANA

Una solución, no solo una integración



Conocimiento

Potencial competitivo

Valor añadido

Insights

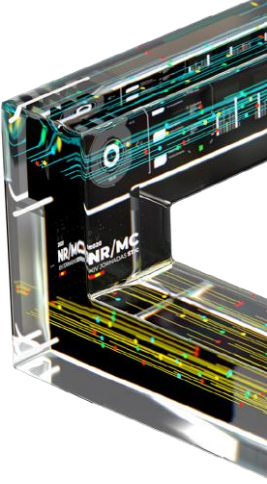
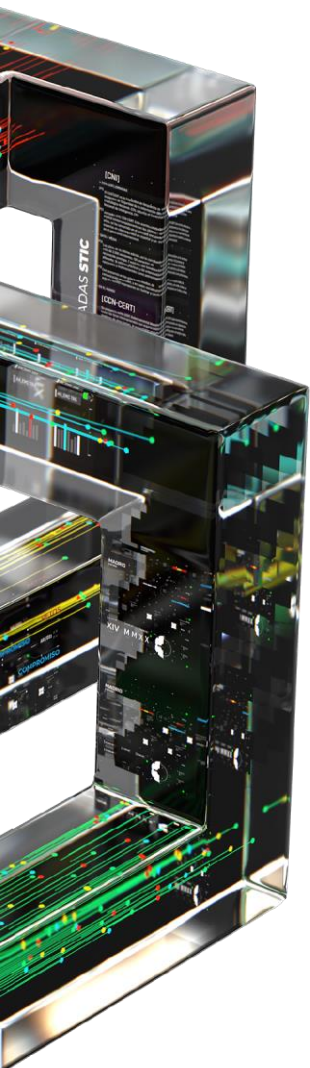
11. Contacto ANA / EMMA



emma@ccn-cert.cni.es
www.ccn-cert.cni.es



ana@ccn-cert.cni.es
www.ccn-cert.cni.es



MUCHAS GRACIAS

#XIVJORNADASCCNCERT