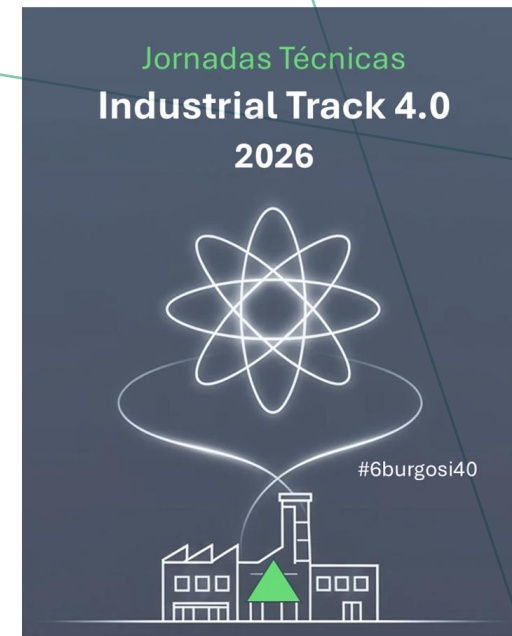


Jornadas Técnicas Industrial Track 4.0 2026

BURGOS, 14 DE OCTUBRE 2026

axians



NORMATIVA DE CIBERSEGURIDAD PARA LA INNOVACIÓN E INDUSTRIA 4.0

ADOLFO GARCÍA YAGÜE – BDM CIBERSEGURIDAD

Brevemente

Trayectoria ligada a la tecnología

- **Trayectoria y puesto actual:** Soy BDM de Ciberseguridad en **Axians**. Cuento con más de 35 años de experiencia en el sector TI, desarrollada en diferentes fabricantes e integradores y vinculada a tecnologías LAN, transporte óptico para operadores, radio, OT/IoT y ciberseguridad
- **Ciberseguridad:** Actualmente desarrollo mi actividad en el ámbito de la ciberseguridad, con especial foco en la protección de infraestructuras en entornos IT/OT/IoT/IoMT y criptografía PQC y QKD
- **Startups OT e innovación IoT:** Participé en la creación de **Energy Minus+** en 2012, compañía española orientada al análisis de datos para lograr eficiencia energética y colaboré en iniciativas de sensorización y telemetría aplicada a movilidad, entre ellas **Telefónica Yamaha Globalrider** (2016)



Innovación + Ciberseguridad + Normativa = Producto

Normativa que debemos conocer

RGPD, ISO 27001, NIS2, ENS, IEC 62443, CRA y EU IA ACT...

- ❑ **RGPD.** Aplicable a cualquier organización que trate datos personales de **ciudadanos de la UE**
- ❑ **ISO 27001. Gestión de la seguridad de la información (SGSI).** Cualquier organización pública o privada
- ❑ **NIS2.** Entidades esenciales e importantes de **sectores críticos ámbito europeo**
- ❑ **ENS (Esquema Nacional de Seguridad).** Seguridad de sistemas y servicios digitales. **Administraciones Públicas españolas y proveedores** que les prestan servicios
- ❑ **IEC 62443.** Ciberseguridad industrial y protección de sistemas de automatización y control. **Operadores industriales, fabricantes e integradores de sistemas OT**
- ❑ **CRA (Cyber Resilience Act).** Seguridad por diseño durante todo el ciclo de vida del producto empleado en Europa. **Fabricantes y proveedores de productos digitales conectados**
- ❑ **EU AI Act.** Gobernanza, gestión de riesgos y uso seguro de la inteligencia artificial. **Proveedores, desarrolladores y usuarios de sistemas de IA en la UE**

Cobertura de dominios de ciberseguridad

ISO 27001, NIS2, ENS, IEC 62443, CRA y EU IA ACT...

Dominio y áreas	Descripción breve	ISO 27001	NIS2	ENS	IEC 62443	CRA	AI Act
Gobierno y gestión de riesgos	Políticas, responsabilidades, gestión de riesgos y cumplimiento normativo	● ●	● ●	● ●	● ●	● ●	● ●
Inventario y visibilidad	Identificación, clasificación y seguimiento de activos IT, OT e IoT	● ●	● ●	● ●	● ●	●	—
Gestión de identidades humanas y máquina	IAM, MFA, PAM, RBAC, identidad de dispositivos y mínimo privilegio	● ●	● ●	● ●	● ●	● ●	●
Criptografía y protección de la información	Certificados, gestión de claves, cifrado e identidad digital de equipos	● ●	● ●	● ●	● ●	● ●	●
Desarrollo seguro y Security by Design	Secure SDLC, Security by Design, DevSecOps y gestión de vulnerabilidades	● ●	● ●	● ●	● ●	● ●	● ●
Seguridad de dispositivos y firmware	Secure Boot, Root of Trust, firmware firmado, integridad y hardening	●	● ●	● ●	● ●	● ●	—
Segmentación OT	Zonas y conduits, DMZ industrial y microsegmentación	●	●	●	● ●	—	—
Gestión de vulnerabilidades	Gestión de CVEs, remediación, actualizaciones y configuración segura	● ●	● ●	● ●	● ●	● ●	● ●
Monitorización y respuesta a incidentes	Detección, notificación, trazabilidad y respuesta a incidentes	● ●	● ●	● ●	● ●	●	● ●
Cadena de suministro y terceros	Gestión de proveedores, componentes software, SBOM y riesgos asociados	● ●	● ●	● ●	● ●	● ●	●
Gestión del ciclo de vida del producto	Actualizaciones seguras, soporte, EOL, mantenimiento y retirada	●	● ●	●	● ●	● ●	● ●
Gobernanza y seguridad de la IA	Gestión de riesgos, transparencia, trazabilidad y supervisión humana	—	—	—	—	—	● ●

Valoración orientativa. La tabla muestra la relación de cada marco con distintos dominios de ciberseguridad: — No contemplado específicamente. ● Relación indirecta. ● ● Requisito explícito

Innovación y desarrollo de soluciones OT

Conviene contemplar la normativa en el ciclo de diseño de un producto

- ❑ No olvides que para pasar de un prototipo a un producto o servicio hay un camino: Dispositivo basado en una MCU o microprocesador. **Necesidad de tiempo real**. Comunicaciones **radio**. Consumo **energético**. Robustez, coste de fabricación para **pequeñas series**, envoltorio, mecanizado y presentación. **Marcado CE**, garantía/RMA... canal de distribución...
- ❑ Cuidado con los **puertos de depuración** expuestos en la PCB, JTAG, UART... diseño anti **tamperización**. Software empleado y cadena de suministro. Seguimiento y remediación de **CVEs**. Anti-rollback. **Certificado X.509** por dispositivo. **Firmware firmado**. Criptochip **TPM** o similar. **Secure boot**. Protocolos estandarizados para operación remota... comunicaciones seguras **mTLS**
- ❑ Arquitectura alrededor de la solución: **Provisioning**, identidad, **PKI**, gestión, **OTA**, exportación de logs y telemetría. **Almacenamiento de datos**. **Revocación** de dispositivos...



Usuario de soluciones OT e Industria 4.0

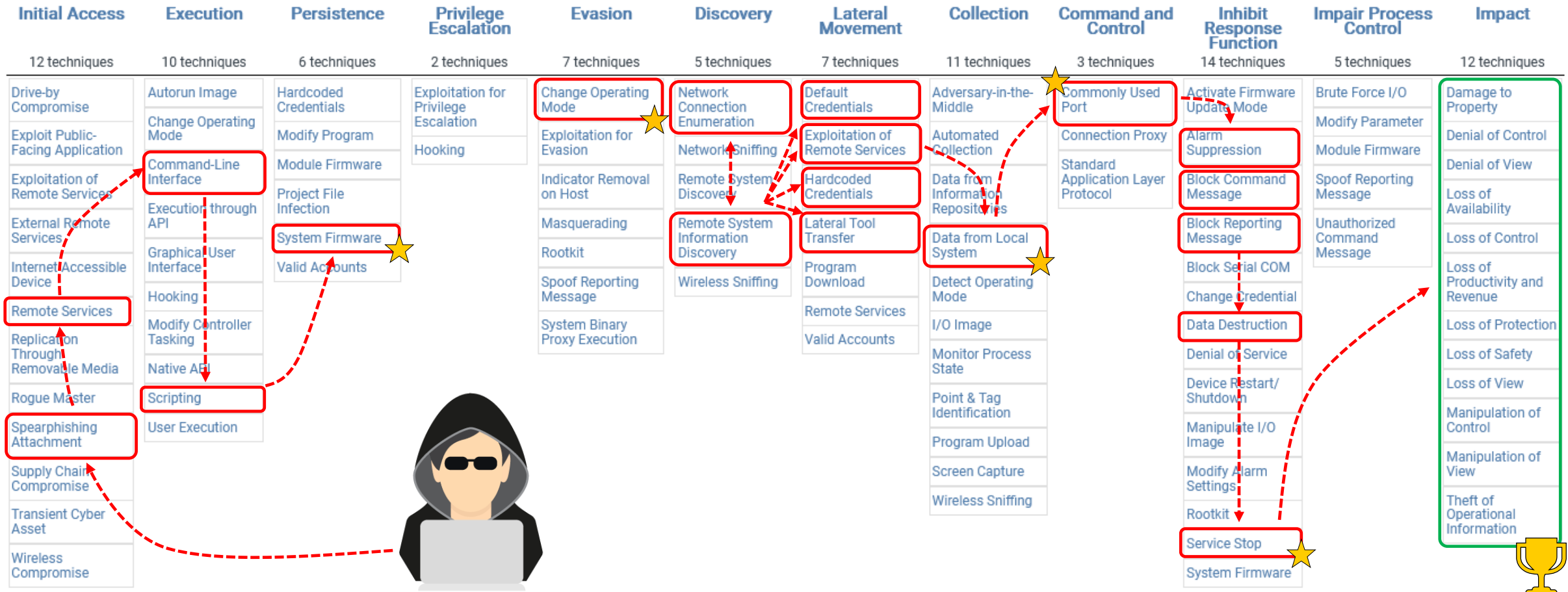
¿Dónde poner el acento para cumplir la normativa?

- ❑ Adquirir soluciones cuyo desarrollo tome en cuenta algún marco normativo para asegurar el **desarrollo seguro, Secure by Design, identidad, cifrado y retención de datos...**
- ❑ Empleo de protocolos seguros basados en **certificados y criptografía asimétrica**. Disponibilidad de mecanismos seguros de provisioning, operación y revocación. Ecosistema de soluciones necesarias: **PKI, almacenamiento, gestión y OTA...**
- ❑ **Acceso remoto y cadena de suministro. Acceso privilegiado. MFA. Inventario y visibilidad de dispositivos. Separación red IT/OT. Segmentación y conduits**
- ❑ **Gobierno de la seguridad. Gestión de riesgos y vulnerabilidades. Respuesta ante incidentes y plan de continuidad. Ciberejercicios. 24x7...**



CRA, NIS2 y IEC 62443

Normativa como herramienta para prevenir y frenar cada fase del ataque



Gracias

axians

+ info en el PI 7