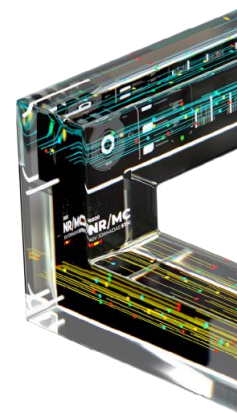


#XIVJORNADASCCNCERT

¿Cómo ATOS sigue los principios del *Charter Of Trust* (CoT) para abordar los problemas de ciberseguridad en la cadena de suministro?



At Atos, our choices impact the world's **digital future.**

"The purpose of Atos is to help design the future of the information technology space in which cybersecurity is a crucial component and enabler.

Our investments in people and leading-edge technologies such as security operating centers, identity and access management, and prescriptive security based on artificial intelligence are key to our success in security.

The Charter is an excellent foundation upon which we can continue to build to spread a trusted, inclusive and sustainable digital economy and create value for our customers and partners."

At Atos, the future is our choice.

Trusted partner for your Digital Journey



Elie Girard, CEO of Atos

¿Cómo ATOS adopta los principios del Chapter of Trust (CoT)?

- CoT establece una serie de Principios Básicos que se deben aplicar de forma estructurada (en cascada) de cara a garantizar la seguridad en la cadena de suministro digital.
- CoT tiene un grupo de trabajo específico para el “Principio 2: “Responsabilidad en toda la cadena de suministro digital” en el que se ha generado una lista de requisitos precisos que se deben aplicar.



Atos está convencido de que la **innovación y colaboración en ciberseguridad de extremo a extremo** es un activo sólido y un diferenciador competitivo para las organizaciones

¿Cómo ATOS adopta los principios del Chapter of Trust (CoT)?

PRINCIPIO 2 - RESPONSABILIDAD

- Se está implementado mediante la modificación de una de nuestras principales Políticas ("Security Requirement for Partner and suppliers"), que se incluye en los contratos con los proveedores, que contiene **una lista de 17 requisitos**, agrupados en las siguientes categorías sobre:

PROTECCIÓN DE DATOS (3)

POLÍTICAS DE SEGURIDAD (3)

RESPUESTA A INCIDENTES (1)

SEGURIDAD DE INSTALACIONES (1)



INTEGRIDAD Y DISPONIBILIDAD (4)

SOPORTE (2)

FORMACIÓN Y CAPACITACIÓN (1)

ACCESO, INTERVENCIÓN, TRANSFERENCIA Y SEPARACIÓN (2)

■ Actively involved
■ Partially involved

DATA PROTECTION 1 <i>Products and services shall be designed to provide confidentiality, authenticity, integrity and availability of data</i> These key principles are not only the foundation of Principle 2 of the Charter of Trust, but are the bedrock of any secure product or service, and should be considered and appropriately implemented early in their design. a. Confidentiality- appropriately protecting data, objects, and resources from unauthorized access, use, or disclosure during processing, storage, and transit. b. Authenticity- assurance that data and products come from the source they claim to be from. c. Integrity- assurance that unauthorized modification to data or products is prevented. d. Availability- assurance that data and products are accessible to authorized parties	SECURITY POLICIES 4 <i>Security policies consistent with industry best practices shall be in effect</i> Mature policies and procedures are critical to provide clear direction to employees on how to operate in a repeatable way, within the confines of an organization's risk tolerance. To that end, organizations should adopt industry best practices that align with standards such as ISO 27001, ISO 20249, SOC2, IEC 62443, or similar trusted standards, to ensure appropriate controls are in place to provide confidentiality, authenticity, integrity, and availability.	INCIDENT RESPONSE 7 <i>For confirmed incidents, timely security incident response for products and services shall be provided to customers</i> Mature incident response policies and procedures are necessary to provide timely response to customers as required by contract, service level agreement, or regulatory requirements.
DATA PROTECTION 2 <i>Data shall be protected from unauthorized access throughout the data lifecycle</i> Data must be protected during all phases of the delivery of a product or service, from creation to destruction, or end of life.	SECURITY POLICIES 5 <i>Guidelines on secure configuration, operation and usage of products or services shall be available to customers</i> Clear and concise directions on how to properly configure, deploy, and operate a product or service are necessary for customers or consumers to fully understand how to secure them.	SITE SECURITY 8 <i>Measures to prevent unauthorized physical access throughout sites shall be in place</i> Mature policies, procedures, and controls are required to prevent unauthorized access to controlled areas such as offices, manufacturing facilities, distribution centers, hosting facilities, labs, etc.
DATA PROTECTION 3 <i>The design of products and services shall incorporate security as well as privacy where applicable</i> The confidentiality and sensitivity of data processed by a product or service must be considered during their design, to ensure appropriate protections are included to prevent unauthorized access, use, or disclosure, and to ensure compliance with any applicable regulatory requirements.	SECURITY POLICIES 6 <i>Policies and procedures shall be implemented so as not to consent to include back doors, malware, and malicious code in products and services</i> Organizations must have Secure Software Development Life Cycle (SSDLC) policies and procedures in place, that can provide reasonable assurances that backdoors, malware, or other malicious code are not included with the product or service, including at the request of a state sponsored actor, criminal organization, or otherwise.	ACCESS, INTERVENTION, TRANSFER & SEPARATION 9 <i>Encryption and key management mechanisms shall be available, when appropriate, to protect data</i> Based on the confidentiality and sensitivity of data stored or processed by a product or service, encryption and key management should be made available for configuration. For example, where data is classified as public, encryption and key management may not be required. However, where data may be classified as confidential, secret, etc., encryption and key management are critical to protect the confidentiality, authenticity, and integrity of the data at rest, in use, and in transit.
CAPABILITY OF MITIGATING RISKS TO SERVICE ENVIRONMENTS Policies and procedures in three key areas are necessary to ensure the confidentiality, integrity, and availability of data and products.	SECURITY POLICIES 16 <i>Measures to prevent unauthorized access throughout sites shall be in place</i> Mature policies, procedures, and controls are required to prevent unauthorized access to controlled areas such as offices, manufacturing facilities, distribution centers, hosting facilities, labs, etc.	SECURITY POLICIES 17 <i>Measures to prevent unauthorized access throughout sites shall be in place</i> Mature policies, procedures, and controls are required to prevent unauthorized access to controlled areas such as offices, manufacturing facilities, distribution centers, hosting facilities, labs, etc.

¿Cómo ATOS adopta los principios del **Chapter of Trust (CoT)**?

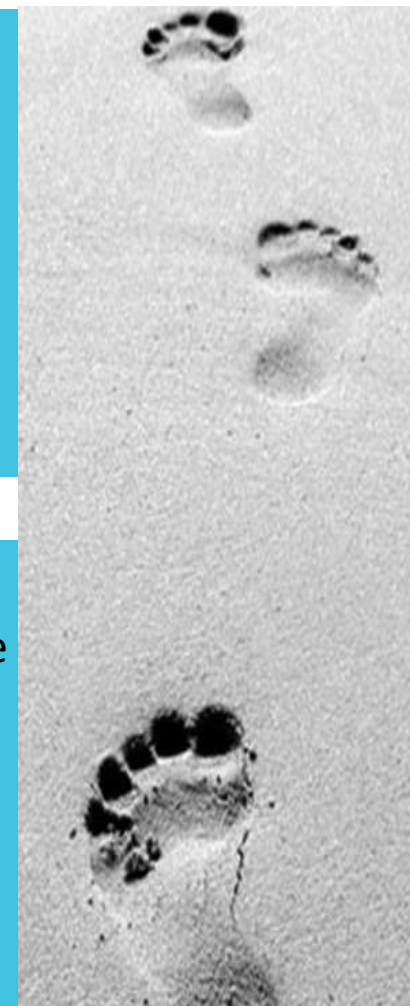
Main insights

PROTECCIÓN DE DATOS

- Los productos y servicios deberán estar diseñados para brindar confidencialidad, autenticidad, integridad y disponibilidad de los datos.
- Los datos se protegerán del acceso no autorizado durante todo su ciclo de vida.
- Se incorporará la seguridad y la privacidad en el diseño de productos y servicios, cuando le sea aplicable.

POLÍTICAS DE SEGURIDAD

- Deberán estar vigentes políticas de seguridad consistentes con las mejores prácticas de la industria.
- Se pondrá a disposición de los clientes, las directrices sobre configuración, funcionamiento y uso seguros de productos o servicios.
- Se implementarán políticas y procedimientos para no permitir la inclusión de puertas traseras, malware y código malicioso en productos y servicios.



¿Cómo ATOS adopta los principios del **Chapter of Trust (CoT)**?

Main insights

RESPUESTA A INCIDENTES

- Para incidentes confirmados, se proporcionará a los clientes una respuesta oportuna para productos y servicios.

SEGURIDAD DE LAS INSTALACIONES

- Deben existir medidas para prevenir el acceso físico no autorizado en todas las ubicaciones.

INTEGRIDAD Y DISPONIBILIDAD

- Se realizarán análisis de seguridad regulares, pruebas y corrección de productos, servicios e infraestructura subyacente.
- Se deben implementar políticas de gestión de activos, gestión de vulnerabilidades y gestión de cambios que sean capaces de mitigar los riesgos en los entornos de servicio.
- Se establecerán procedimientos de continuidad del negocio y recuperación ante desastres e incorporarán la seguridad durante la interrupción, en caso de producirse.
- Deberá existir un proceso para garantizar que los productos y servicios sean auténticos e identificables.



Main insights

- Los mecanismos de cifrado y gestión de claves deberán estar disponibles, cuando sea apropiado, para proteger los datos.
- Se establecerá y se hará cumplir el nivel adecuado de control y supervisión de la identidad y el acceso, incluidos terceros.

- Se debe definir y comunicar adecuadamente el período de soporte, especificando la vida útil prevista de los productos, servicios o soluciones.
- Basados en el riesgo, y durante el período de tiempo del soporte, se implementarán procesos para: (1) Contactar con el soporte, (2) Avisos de seguridad, (3) Gestión de vulnerabilidades y (4) Entrega y soporte de parches relacionados con ciberseguridad.

- Se debe implementar regularmente un nivel mínimo de formación y capacitación en seguridad para los empleados (por ejemplo, mediante certificaciones, concienciación).



¿Cómo ATOS adopta los principios del Chapter of Trust (CoT)?

Category	Baseline Cybersecurity Supply Chain Requirements ¹⁾	Mapping against standards				
		IEC 62443	ISO 27001	ISO 20243	NIST CSF	METI CPSF
Data Protection	Products or services shall be designed to provide confidentiality, authenticity, integrity and availability of data	✓	✓	✓	Partially addressed	Partially addressed
	Data shall be protected from unauthorized access throughout the data lifecycle	✓	✓	✓	✓	✓
	The design of products and services shall incorporate security as well as privacy where applicable	✓	✓	Partially addressed	Not in scope	Partially addressed
Security Policies	Security policies consistent with industry best practices such as ISO 27001, ISO 20243, SOC2, IEC 62443 shall be in effect ²⁾	✓	✓	✓	Partially addressed	✓
	Guidelines on secure configuration, operation and usage of products or services shall be available to customers	✓	Not in scope	Partially addressed	Not in scope	Not in scope
	Policies and procedures shall be implemented so as not to consent to include back doors, malware, and malicious code in products and services.	✓	✓	✓	✓	✓
Incident Response	For confirmed incidents, timely security incident response for products and services shall be provided to customers	✓	✓	✓	✓	✓
Site Security	Measures to prevent unauthorized physical access throughout sites shall be in place	✓	✓	✓	✓	✓
Access, Inter-vention, Transfer & Separation	Encryption and key management mechanisms shall be available, when appropriate, to protect data	✓	✓	✓	✓	✓
	Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced	✓	✓	✓	✓	✓
Integrity and Availability	Regular security scanning, testing and remediation of products, services, and underlying infrastructure shall be performed	✓	✓	✓	✓	✓
	Asset Management, Vulnerability Management, and Change Management policies shall be implemented that are capable of mitigating risks to service environments	✓	✓	Partially addressed	✓	✓
	Business continuity and disaster recovery procedures shall be in place and shall incorporate security during disruption, where applicable	✓	✓	✓	Partially addressed	✓
	A process shall be in place to ensure that products and services are authentic and identifiable	✓	Not in scope	✓	Partially addressed	Partially addressed
Support	The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available	✓	Not in scope	✓	✓	✓
	Based on risk, and during the timeframe of support, processes shall be in place for: (1) Contacting Support, (2) Security Advisories, (3) Vulnerability Management, and (4) Cybersecurity related Patch Delivery and Support	✓	✓	✓	✓	✓
Training	A minimum level of security education and training for employees shall be regularly deployed (e.g., by training, certifications, awareness)	✓	✓	✓	✓	✓

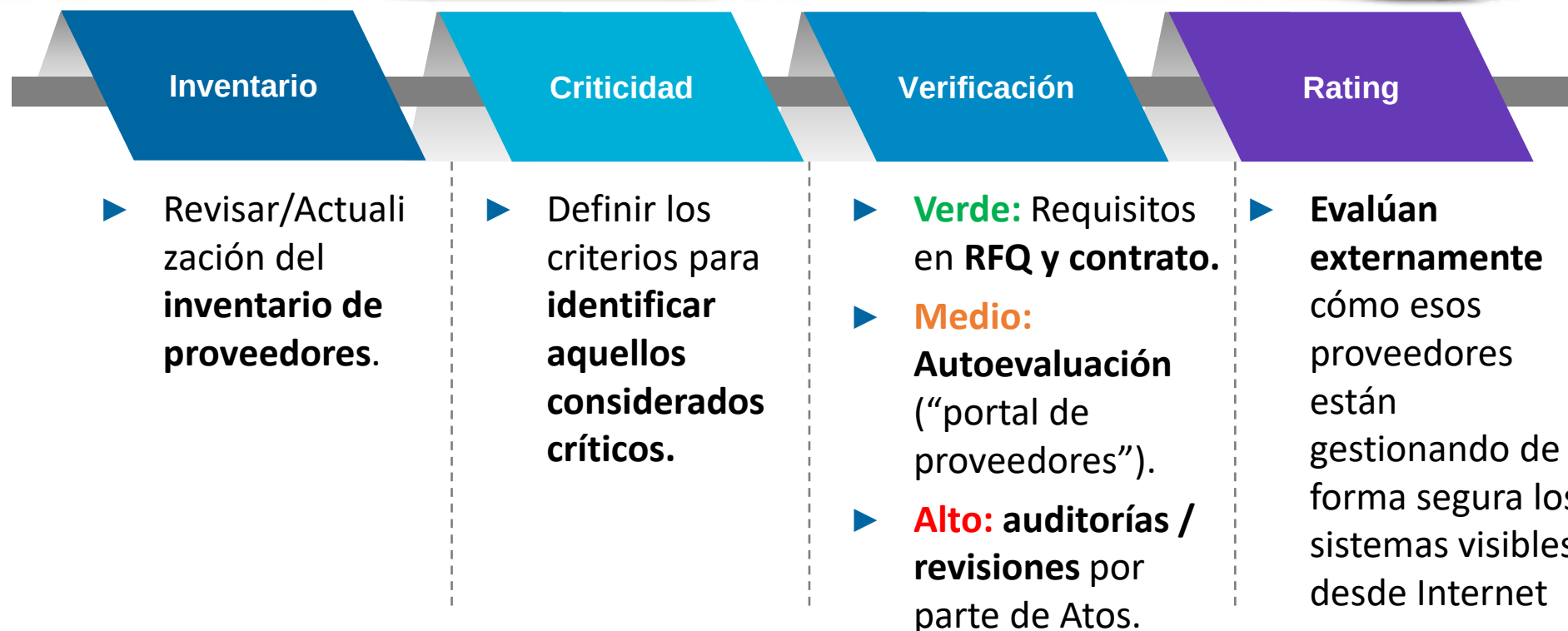
1) For next generation products and solutions

2) Including access control, security education, employment verification, encryption, network isolation/segmentation, operational security, physical security, vendor management

¿Cómo ATOS adopta los principios del Chapter of Trust (CoT)?

PROVEEDORES Y TERCERAS PARTES

- ▶ En una empresa tan grande como Atos, la lista de proveedores también es igualmente extensa y la revisión sistemática consumiría un alto nivel de recursos. El **enfoque actual** se está llevando a cabo de una manera **pragmática**:



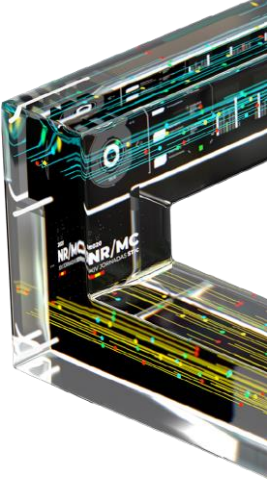
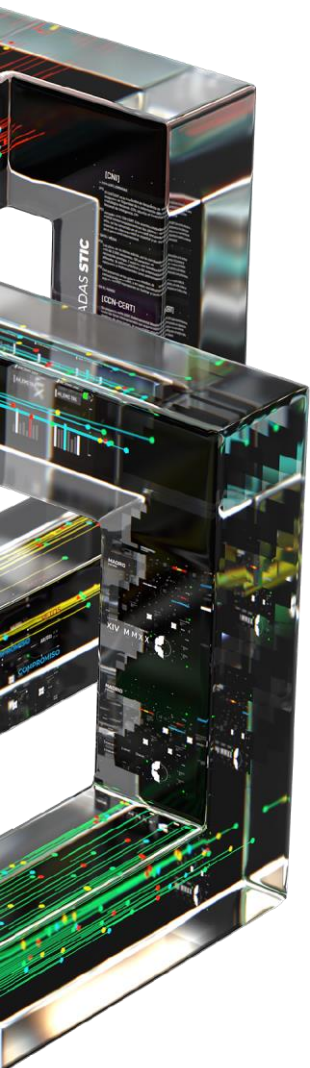
More information - atos.net

Contact: arancha.jimenez@atos.net



Trusted partner for your **Digital Journey**

Atos



MUCHAS GRACIAS

#XIVJORNADASCCNCERT