Estado del Arte de Safety & Security

XUNTA DE GALICIA | igape

Oportunidades Industria 4.0 en Galicia

Convenio de colaboración entre el Instituto Gallego de Promoción Económica, la Alianza Tecnológica Intersectorial de Galicia y los centros integrantes de esta alianza para la detección y análisis de oportunidades sectoriales para las empresas industriales gallegas en el ámbito de la industria 4.0

AtiGA ALIANZA TECNOLÓGICA INTERSECTORIAL DE GALICIA | aimen CENTRO TECNOLÓGICO | ANFACO CECOPESCA | CTAG Centro Tecnológico de Automoción de Galicia | energylab | gradiant | instituto tecnológico de galicia

ÍNDICE

1. INTRODUCCIÓN

"The physical and virtual worlds are increasingly merging together. A growing number of physical objects have intelligent sensor and actuator technology and are being networked through the development of the Internet of Things. The availability of all relevant information in real time through the networking of all instances involved in value creation, as well as the ability to derive the best possible value stream from data at any time is triggering the next stage of the industrial revolution known as Industrie 4.0." [1]

La industria manufacturera está pasando por grandes cambios. La cuarta revolución, impulsada por el Internet de las Cosas, está ocurriendo. Está creando **redes inteligentes** -conectando máquinas, trabajadores y sistemas- que pueden intercambiar información de manera automática, activar acciones y controlarse de forma autónoma. Se estima que el 85% de las empresas habrán implementado soluciones de Industria 4.0 en todas las divisiones de negocios importantes dentro de cinco años. En 2020 representará 140 mil millones de euros gastados anualmente en Europa[2].

La fabricación es un objetivo altamente lucrativo para los ataques, que van desde el espionaje cibernético, robo de la propiedad intelectual hasta sabotaje de las plantas industriales. Sin embargo, los fabricantes no necesitan desesperarse ya que es posible **securizar todos los sistemas TI (Tecnologías de la Información)** y sus procesos. Alcanzar una resiliencia cibernética implica diligencia, buena práctica y gestión de riesgos que estén soportados por una correcta estrategia de seguridad y tecnología. Con estas estrategias establecidas, los fabricantes aumentarán su éxito y competitividad aprovechando todo lo que la Industria 4.0 ofrece.

Aunque es cierto que existe un beneficio en la integración de sistemas que antes estaban separados, también acarrea **riesgos para la seguridad**. Procesos que antes estaban aislados, son ahora vulnerables a los ciberataques, tanto directamente como indirectamente.

El cambio está ocurriendo en toda la industria manufacturera. La necesidad de aumentar la agilidad y la flexibilidad ha creado la Industria 4.0, la "Internet Industrial", donde todo, desde las líneas de ensamblaje hasta los camiones de reparto están interconectados vía Internet. En esta cuarta revolución industrial, la fusión de los mundos físicos y virtuales en una red global de sistemas ciberfísicos está cambiando rápidamente el control de la producción. Mientras esto **trae beneficios** -en costes más bajos y mayor eficiencia- también **aumenta los riesgos**. La complejidad de la gestión de la producción y de la red de proveedores a través de la cadena de valor crece enormemente. Es un reto para que los cibercriminales lo exploten.

Lo desafíos del Internet Industrial intensifican la amenaza de **daños causados por los ciberataques**. Pueden causar alteraciones o largas paradas con un enorme coste. Como demuestra un reciente cuestionario de Deloitte[3], los fabricantes creen que los potenciales ciberriesgos aumentan de modo significativo con la transformación a la Industria 4.0.

---

[1] "Implementation Strategy Industrie 4.0 - Report on the results of the Industrie 4.0 Platform". 2016. Bitkom, VDMA, ZVEI. http://www.zvei.org/Publikationen/Implementation-Strategy-Industrie-40-ENG.pdfhttp://www.zvei.org/Publikationen/Implementation-Strategy-Industrie-40-ENG.pdf

[2] Deloitte: Industry 4.0 Challenges and Solutions for the digital transformation and use of exponential technologies

[3] Deloitte: Global Cyber Executive Briefing: Manufacturing

El **Departamento de Seguridad Nacional de Estados Unidos**[4] informó que los ataques cibernéticos en el sector manufacturero casi se duplicaron en un año. Este aumento de los incidentes de seguridad hizo aumentar las pérdidas financieras un 38% con respecto al año anterior, según el estudio de PwC 'The Global State of Information Security Survey 2015 – Industry'. Además la convergencia del TI Operacional (OT- Operational IT) y la tradicional TI (Office IT) crea un nuevo nivel de riesgo. Una amenaza a TI ya no está aislada y puede convertirse en un problema para los sistemas de OT.

El mensaje es claro: para hacer la transformación digital hacia la Industria 4.0 con seguridad, las empresas manufactureras necesitan **fortalecer activamente**[5] **la gestión del riesgo cibernético**.

1.1 DEFINICIÓN/DESCRIPCIÓN

Entender correctamente las diferencias de *Safety y Security* es esencial para el entendimiento de este estado del arte, por lo que primero se explicarán desde un punto general para luego poder profundizar.

"Safety" se refiere al hecho de que los sistemas tecnológicos (máquinas, productos, instalaciones productivas etc) no deben representar un peligro para la gente o el ambiente, mientras que **"Security"** se refiere a que los sistemas deben estar protegidos contra ataques y accesos no autorizados. Es esencial establecer una distinción clara entre los dos términos:

- **Security/IT security/cyber-security:** La protección de los datos y servicios en los sistemas digitales contra los malos usos. Ej: acceso no autorizado, modificación o destrucción. Los objetivos de las medidas de seguridad son aumentar la confidencialidad (restricción del acceso a datos y servicios), integridad (exactitud, exhaustividad de los datos y correcto funcionamiento de los servicios) y disponibilidad (una forma de medida de la habilidad de los sistemas para realizar una función en un momento particular). "Security" proporciona una línea base para la privacidad de la información, por ejemplo la protección de los datos personales o la protección de know-how.

ILUSTRACIÓN 1: SAFETY & SECURITY

[4] US sees jump in cyber attacks on critical manufacturing infrastructures, report by Jim Finkle

[5] Smarter Security For Manufacturing in the Industry 4.0 ERA - Sysmantec

- **Safety:** Es la ausencia de riesgos y amenazas a las personas y el medio ambiente como consecuencia del funcionamiento del sistema. Puede involucrar aspectos adicionales como la prevención de peligros mecánicos o eléctricos, protección de la radiación, prevención de los riesgos relacionados con válvulas o altas presiones, etc. La seguridad operacional (Operational Safety[6]) se refiere a los aspectos de seguridad que dependen del correcto funcionamiento del sistema o que son proporcionados por el propio sistema. Los elementos necesarios para ofrecer seguridad operativa incluyen bajos índices de fallos, tolerancia a fallos (es decir, la capacidad para seguir operando correctamente incluso cuando ocurren fallos) y robustez (la capacidad de garantizar la funcionalidad básica en caso de fallo). La fiabilidad (Reliability) se refiere a la probabilidad de que un sistema (tecnológico) funcione correctamente durante un período de tiempo dado en un entorno dado.

Además se asocia a los conceptos de *Safety y Security* una serie de **amenazas y riesgos**:

- **Riesgos - Hazards** (*Safety*)
  - Entendibles y con conocimiento de la peligrosidad
  - Predecibles basándose en datos históricos
  - Se pueden crear probabilidades de posibles accidentes

- **Amenazas - Threats** (*Security*)
  - No son totalmente entendibles
  - No son predecibles

[6] Recommendations for implementing the strategic initiative INDUSTRIE 4.0 - Final report of the Industrie 4.0 Working Group

1.1.1 Safety

Históricamente la industria asigna a todo lo relacionado con *Safety* un peso muy importante. Se entiende que los accidentes son previsibles y solo ocurren si se aplica acciones inseguras sobre los sistemas o si no se siguen los procedimientos definidos. Es por eso que el **concepto *Safety* tiene más importancia que *Security* en el entorno industrial**.

Nivel de prioridades TI vs Industria[7]:

PRIORIDAD	TI	INDUSTRIAL
1	Confidencialidad	Integridad
2	Integridad	Disponibilidad
3	Disponibilidad	Confidencialidad

Como se observa, l**as prioridades son totalmente diferentes entre Tecnologías de la Información y el sector Industrial**. Integridad en la industria siempre estará en la pirámide de prioridades, ya que el impacto es muy alto. Además la disponibilidad estará supeditada a la Integridad.

Es importante señalar que los objetivos de la industria tienen un impacto directo en la "*Safety*" de los operarios. Los planes que se deben preparar están relacionados con los siguientes objetivos:

- Rendimiento
- Disponibilidad
- Prioridad de la arquitectura con respecto a la información
- Interacción física
- Respuestas críticas en tiempo
- Operaciones
- Tiempo de vida de los sistemas
- Acceso a componentes

Los sistemas destinados a ello son una contramedida crucial para las plantas, y se utilizan para proteger la salud humana, vegetal y el medio ambiente en el caso de que el proceso vaya más allá de los márgenes de control. No se controla el proceso en sí mismo, sino más bien la protección. Para ello se utilizan los **sistemas de control de proceso (PCS)** que están interconectados con los sistemas de seguridad para que se tomen acciones inmediatas en caso de que los PCS fallen.

Los sistemas de control de proceso y de *Safety* están unidos bajo un mismo sistema llamados **Sistema de seguridad (ICSS)** y **Control Integrado**. Los sistemas de *Safety* industrial suelen utilizar sistemas dedicados **que son SIL 2 (Safety Integrity Level),** mientras que los sistemas de control pueden comenzar con SIL 1.

[7] Infraestructuras críticas y sistemas industriales - Juan Francisco Bolívar

Además, se suele usar los **SIL (Safety Integrity Level)** que definen **Probability of Failure on Demand (PFD)** y risk reduction factor (RRF) (IEC EN 61508)

Safety Integrity Level	Safety	Probability of Failure on Demand	Risk Reduction Factor
SIL 4	> 99.99%	0.001% to 0.01%	100,000 to 10,000
SIL 3	99.9% to 99.99%	0.01% to 0.1%	10,000 to 1,000
SIL 2	99% to 99.9%	0.1% to 1%	1,000 to 100
SIL 1	90% to 99%	1% to 10%	100 to 10

ILUSTRACIÓN 2: NIVELES DE RIESGO Y FALLO SIL

Hay tres **tipos principales de sistemas** de *Safety* en la industria de procesos:

1. Sistema de **proceso de seguridad o sistema de proceso de cierre (PSS).**
2. Sistema de **apagado de emergencia (SSS).** Compuesto de un sistema de desconexión de seguridad (SSS) que deberá modificar las instalaciones a un estado seguro en caso de una situación de emergencia. El sistema de desconexión de seguridad asumirá la gestión de todas las entradas y salidas relativas a la función de parada de emergencia (ESD).
    a. **Parada de Emergencia (ESD)**:
        i. EDS Nivel 1: A cargo del apagado general del área de la planta, puede activar el nivel 2 de ESD. Este nivel solo se puede activar desde la sala de control principal en las plantas industriales de proceso.
        ii. EDS Nivel 2: Este nivel cierra y aísla las zonas de EDS individuales y activa si es necesario EDP.
        iii. EDS Nivel 3: Proporciona “inventario de contención de líquidos”.
    b. **Despresurización (EDP)**: Se utilizan para liberar fluidos peligrosos, por ejemplo en las tuberías después de un cierre de válvulas.

1.1.2 Security

ILUSTRACIÓN 3: CRECIENTE EVOLUCIÓN E IMPACTO DE LOS ATAQUES INFORMÁTICOS

La seguridad es uno de los temas más relevantes en las industrias de hoy en día debido a que manejan **sistemas críticos**. Existe un incremento del interés en la seguridad en sistemas industriales debido a una serie de eventos, desde el incremento del número de vulnerabilidades publicadas afectando a estos sistemas -como se representa en la siguiente figura donde se puede ver un aumento casi exponencial- hasta un mayor número de herramientas de fácil uso que deriva en un crecimiento de los ataques. Además, por parte de la industria existe una mayor concienciación de seguridad mientras que el ecosistema comercial usa **la seguridad como un factor diferenciador** de sus productos.

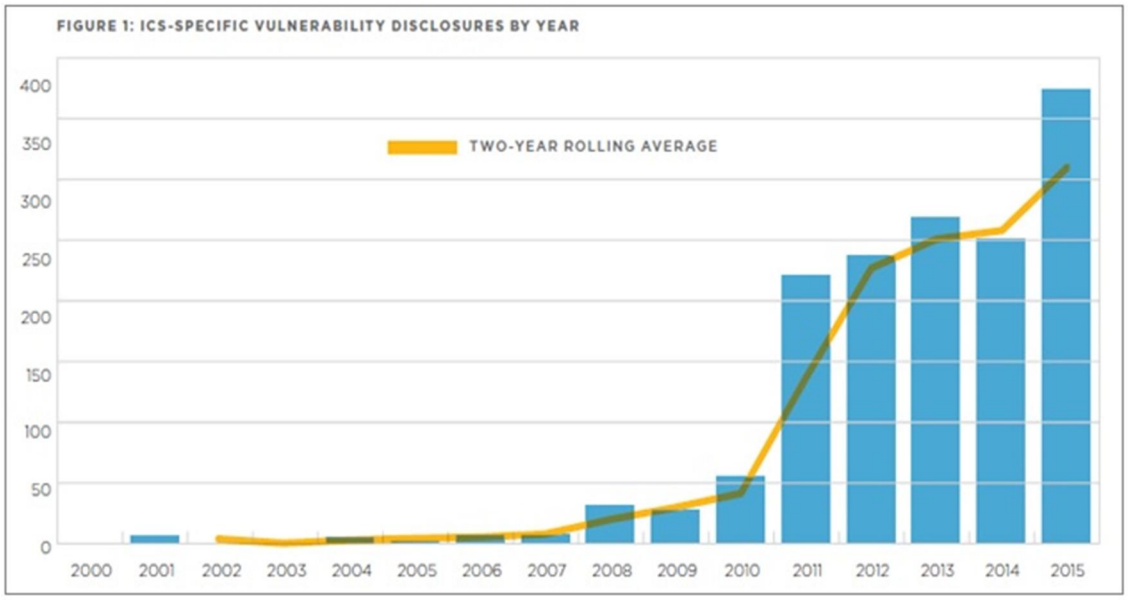


ILUSTRACIÓN 4: VULNERABILIDADES REVELADAS POR AÑO EN ENTORNOS INDUSTRIALES[8]

[8]FireEye 2016 ICS Vulnerabilities Trend Report: Missed Warnings, Exposed Industrial Environments

Los **desafíos del Internet Industrial** aumentan la amenaza de daños causados por ataques cibernéticos que manipulan los sistemas de procesamiento y flujo de trabajo. Pueden causar perturbaciones o interrupciones a un coste enorme.

Es normal ver ataques dirigidos contra el sector manufacturero por parte de **hackers y ciberdelincuentes.** Los ataques van desde tácticas de delincuencia cibernética, robo de datos confidenciales y la propiedad intelectual sobre nuevos diseños y productos, hasta el sabotaje cibernético de procesos industriales o el centro de datos de TI.

Existe una variedad de **activos digitales propensos a ser atacados** en entornos de sistemas de control como por ejemplo:

- Dispositivos de Redes.
- Controladores lógicos programables.
- Interfaz hombre-máquina.
- Sensores de adquisición de datos.
- Unidades de control remoto.
- Estaciones de trabajo.
- Servidores.

Además como se muestra en las siguientes figuras, aún queda mucho trabajo por hacer por parte de las organizaciones y desarrolladores para **securizar todos los servicios** implantados en sistemas críticos.

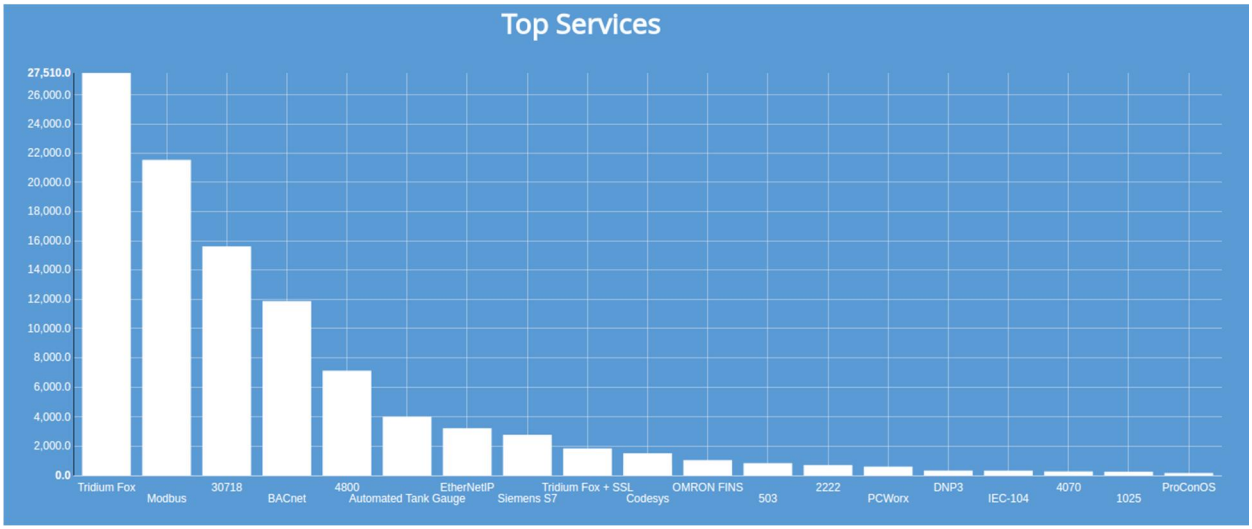


ILUSTRACIÓN 5: SERVICIOS INDUSTRIALES EXPUESTOS A INTERNET[9]

[9] Industrial Control Systems - Shodan

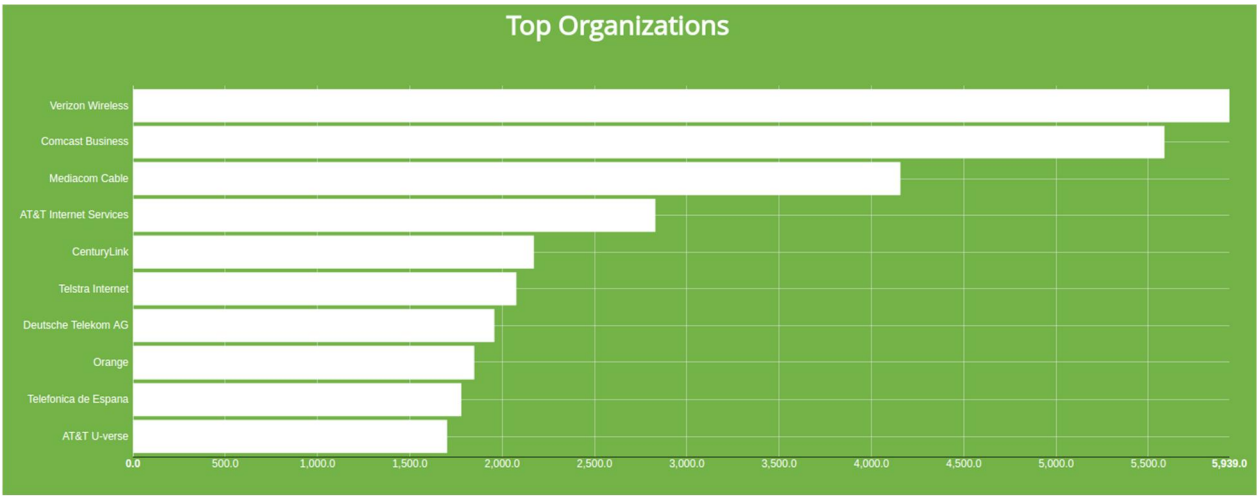


ILUSTRACIÓN 6: ORGANIZACIONES QUE GESTIONAN ESTOS PRODUCTOS

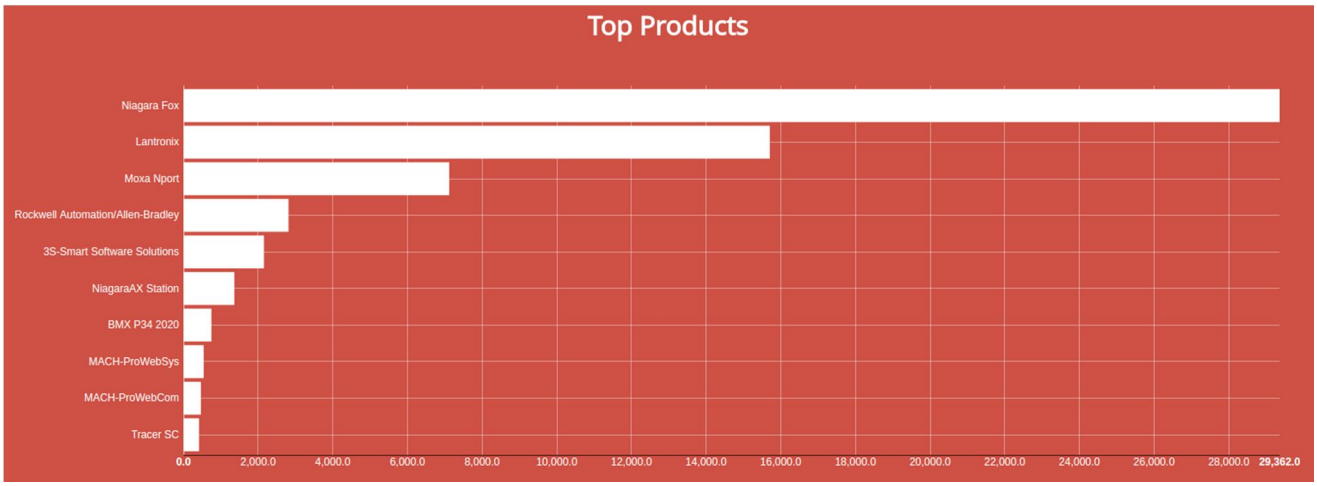


ILUSTRACIÓN 7: PRODUCTOS MÁS USADOS EN ICS

A raíz de estos activos digitales, las **vulnerabilidades más habituales** se suelen encontrar en:

- Uso de funciones inseguras en aplicaciones ICS.
- Servicios web.
- Implementación de los protocolos de red.
- Actualizaciones de sistemas.
- Autenticación débil.
- Violación de permisos.
- Divulgación de información.
- Diseño de red insegura.
- Malas configuraciones, en general de red.

Todos estos ataques los protagonizan una serie de actores con diversos propósitos. Desde empleados descontentos, hasta organizaciones gubernamentales con motivaciones de espionaje o simplemente investigadores con ataques como pruebas de concepto.

ILUSTRACIÓN 8: TAXONOMÍA DE LOS POSIBLES ACTORES EN CIBERAMENAZAS

1.1.3 Cyber Kill Chain

Estos actores se basan en prácticas militares para alcanzar sus objetivos. Esta técnica se le conoce como Cyber Kill Chain. El concepto Cyber Kill Chain fue acuñado por analistas de *Lockheed Martin Corporation*. En el año 2011 publicaron un artículo donde explicaban lo que llamaban **Intrusion Kill Chain**[10], con la intención de ayudar a la toma de decisiones para detectar y responder de una forma más adecuada a los posibles ataques o intrusiones a los que se encuentra expuesto cualquier sistema.

[10] Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

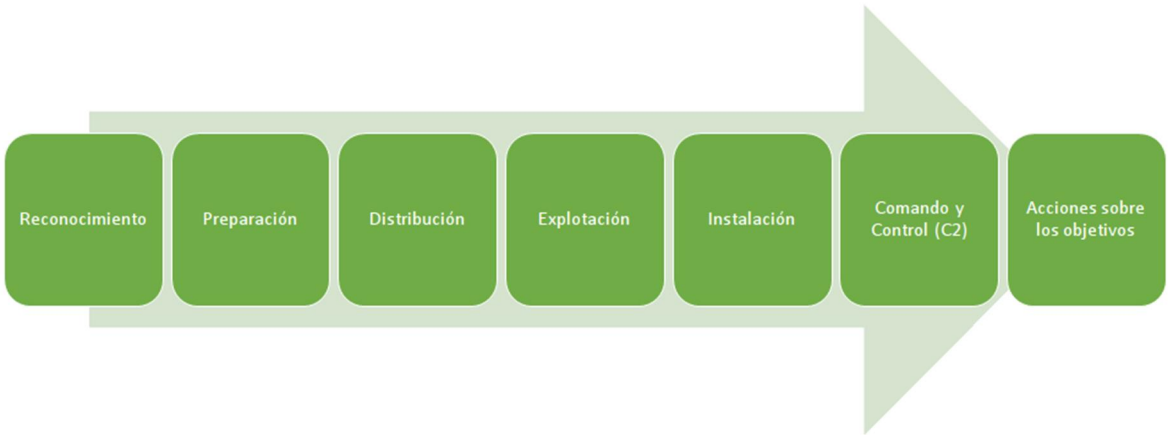


ILUSTRACIÓN 9: CYBER KILL CHAIN

- **Reconocimiento**
  - Obtención de información técnica (DNS, IP, puertos)
  - Obtención de información de empleados (nombres, teléfonos, correos electrónicos,…). Por ejemplo, redes sociales.
  - Detección de vulnerabilidades (enumeración de servidores, escaneo de vulnerabilidades)
  - Todo ocurre en el lado del atacante, para algunas técnicas ni siquiera es necesario acceder a los sistemas de la víctima.

- **Preparación**
  - El atacante usa un software que explota una vulnerabilidad (exploit) y crea un programa malicioso asociado para enviar a la víctima.
  - El programa se diseña específicamente para la víctima (spearphising, esquivar A/V,…)
  - Todo ocurre en el lado del atacante.

- **Distribución**
  - El programa malicioso se entrega a la víctima.
  - Existen multitud de vías de entrega: spearphising, USB, water hole, servidores web, …)
  - El atacante protegerá su identidad: VPN, proxy, red TOR,…
  - Uno de los puntos principales de detección por parte de la víctima.

- **Explotación**
  - Ejecución del programa enviado a la víctima.
  - Se aprovecha de una vulnerabilidad software o de un error humano (engaño) para su ejecución.

- **Instalación**
  - Se instala malware en el ordenador o servidor infectado.
  - Se asegura que la instalación sea permanente.
  - Se asegura que el malware no sea detectado.

- **Comando y Control (C2)**
  - El malware se comunica con su central.
  - Proporciona a los atacantes control remoto y capacidad para extraer datos.
- **Acciones sobre los objetivos**
  - Se procede al robo o a la ejecución de lo que se planteara hacer.
  - Este paso puede llevar meses o años (ataque persistente).

1.2 FUNDAMENTOS DE SEGURIDAD

Como se explicó en "Implementation Strategy Industrie 4.0", un informe publicado en abril 2015 por Industrie 4.0, el intercambio de información a través de toda la cadena de valor es esencial para la Industria 4.0. Un intercambiador de información securizado requiere de **identificación única** y **autenticación** de los individuos, procesos y máquinas, y la **verificación de ciertas propiedades.**

Las identidades seguras son el punto inicial para la cadena de seguridad que protege la captura de datos, transporte y procesado. El primer objetivo de las identidades seguras es empezar en una cadena de confianza en unas comunicaciones automatizadas. Estas se soportan en tres objetivos bien conocidos:

- **Confidencialidad:** Garantiza el nivel de secreto necesario en cada parte del procesado de datos y previene de la revelación no autorizada. Debe protegerse donde está almacenada y en tránsito.
- **Integridad:** Garantizar la exactitud y fiabilidad de la información y de los sistemas, de esta manera se evitan modificaciones no autorizadas. Cuando se instala un malware en un sistema se compromete su integridad. Esto puede provocar la corrupción, modificación maliciosa o cambio por información incorrecta. Controles de acceso estrictos, detección de intrusión y hashing pueden combatir estas amenazas.
- **Disponibilidad:** Garantiza el acceso fiable y adecuado en el tiempo a recursos e información a usuarios autorizados. Las aplicaciones, servidores etc deben garantizar un acceso con el rendimiento adecuado, recuperarse de cortes de servicio de una manera segura y adecuada. Es complejo al haber una gran variedad de arquitecturas (comunicaciones, sistemas, bbdd, aplicaciones...)

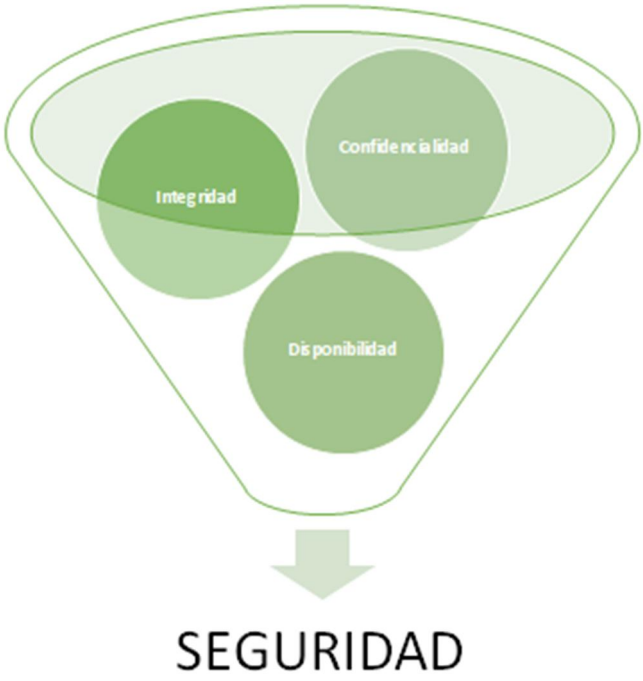


ILUSTRACIÓN 10: OBJETIVOS DE SEGURIDAD

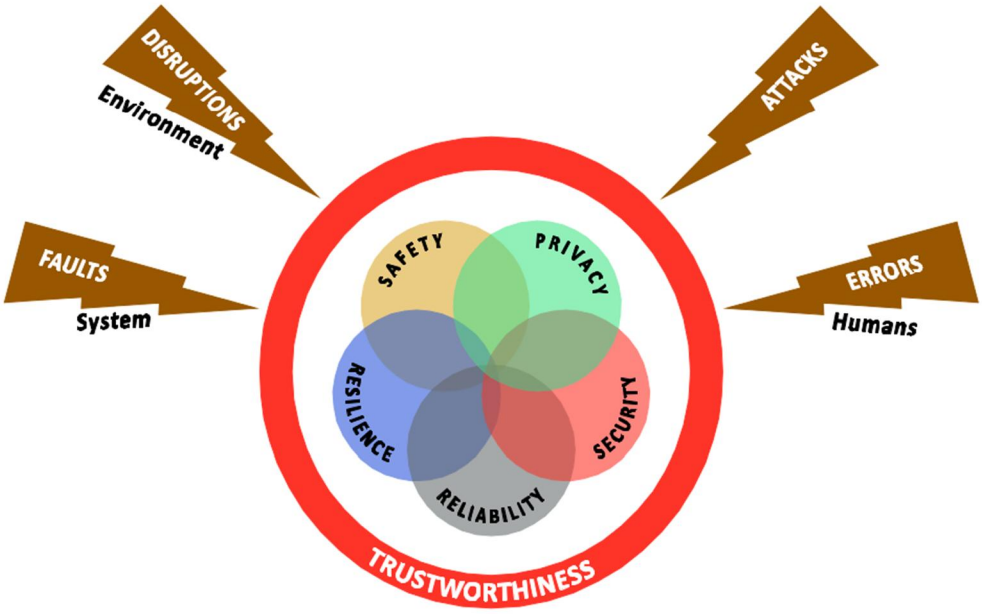
Ejemplificándolo, se puede comparar con el **control de un portero para acceder a un edificio**. Por ejemplo, el portero chequea sobre la base datos de autorizaciones de la compañía para entrar en el edificio. El portero comprueba la autenticidad y la validez del ID de la compañía y hace una validación cruzada del usuario en una blacklist. Después compara la persona con la foto (de su pasaporte, y aplicando características biométricas). En el mundo digital también es necesario verificar a quién se le ha concedido el acceso a los datos o ha hecho un pedido y si esta persona está autorizada para hacerlo. En ambos mundos estos son procesos fundamentales que proveen la base para operaciones exitosas y deben ser conducidos con el debido cuidado.

Las **identidades seguras** también son importantes para los procesos legales y comerciales. En principio, aumentan la transparencia de los procesos. Esto es fácil de entender, quién, cómo, cuándo y con qué derechos alguien se comunica y, posiblemente, decide. En general se puede decir que: cuanto más **fiables (reliable), confiables (trustworthy) y rastreables** sean las identidades, más óptima será la transferencia automatizada de la autoridad de ejecución y de toma de decisiones de personas, máquinas y componentes. De esta manera, las identidades seguras permiten ganar eficiencia.

Un sistema Industrial Internet of Things (IIoT) presenta características de end-to-end, al igual que muchos otros sistemas como por ejemplo **Security Shells**, surgen como resultado de las propiedades de sus diversos componentes y la naturaleza de sus interacciones.

Las cinco **características clave del sistema** que más afectan a las decisiones de confianza de un despliegue son:

- **Security**.
- **Safety**.
- **Fiabilidad (Reliability):** Es la capacidad de un sistema o componente para realizar las funciones requeridas bajo unas condiciones en un periodo específico de tiempo.
- **Resiliencia:** Es la propiedad de un sistema para evitar, absorber y manejar las condiciones dinámicas adversas mientras completa la misión asignada y reconstituye las capacidades operacionales.
- **Privacidad:** Es el derecho de un individuo o grupo para controlar o influenciar qué información relacionada con ellos puede ser recolectada, procesada y almacenada por quién y a quién dicha información puede ser revelada.
- **Sistemas confiables (trustworthy systems):** Uno de los principales objetivos de un sistema es que sea confiable con respecto a las características clave del sistema. La importancia de cada característica para un despliegue dado es única y el logro de uno puede entrar en conflicto con el logro de otro. Estas interacciones deben basarse en el cumplimiento normativo, el proceso empresarial y las normas de la industria, no aisladamente.



El **argot del mundo de la seguridad** es complejo y extenso, pero es importante tener claros los siguientes conceptos:

- **Vulnerabilidad (Vulnerability):** Debilidad de un sistema.
- **Amenaza (Threat):** Peligro potencial asociado a la explotación de una vulnerabilidad.
- **Riesgo (Risk):** Impacto de negocio asociado a la ejecución de una amenaza.
- **Control (Contermeasure/Safeguard):** Elemento que mitiga un riesgo potencial.
- **Activo (Asset):** Elemento de valor para la organización.

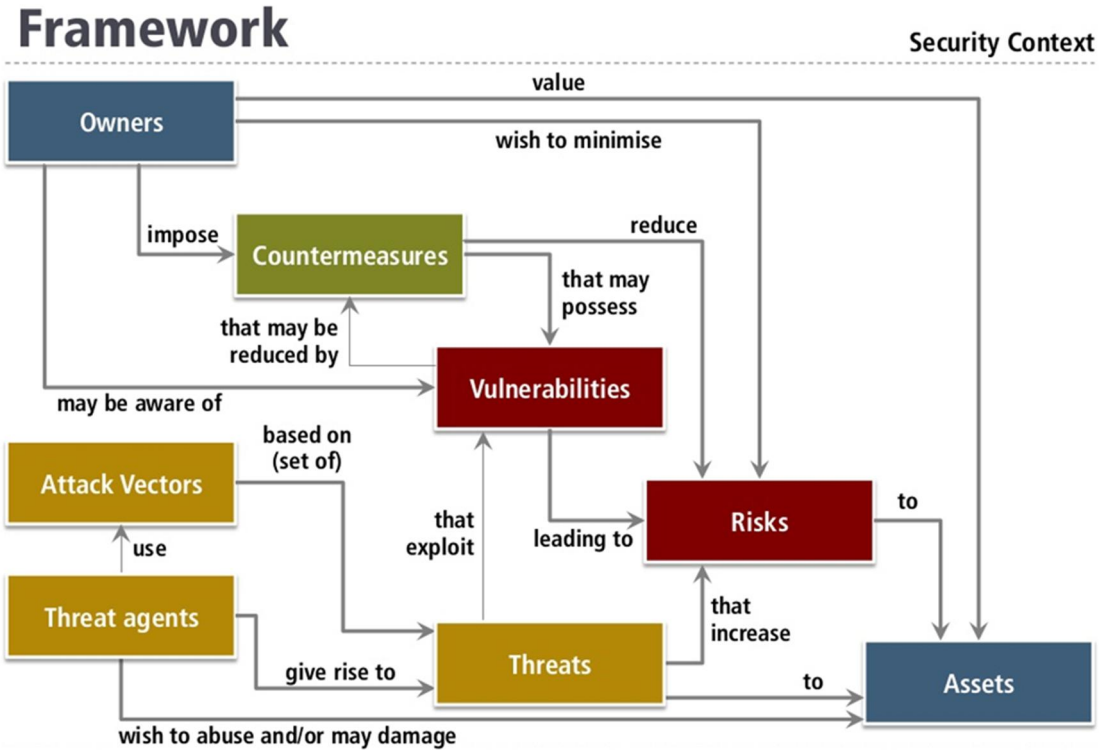


ILUSTRACIÓN 11: LOS ELEMENTOS DE RIESGO Y SUS RELACIONES DE ACUERDO A LA ISO 15408:2005

PRINCIPIO DE PROPORCIONALIDAD

La **regla de oro que el Control Interno Informático** de la organización ha de tener siempre en mente para diseñar e implantar los controles es el principio básico de proporcionalidad. Es decir, deben cuantificarse los siguientes aspectos:

- Coste de diseño.
- Implantación.
- Monitorización.
- Mantenimiento del control.

En general, la seguridad implica **costes incluso más allá del coste de los sistemas**, software o tiempo de expertos en la configuración y diseño de los mismos. También tiene un coste en la forma de la resistencia de los empleados o su frustración, que en ocasiones ven las medidas de seguridad como impedimentos para realizar su trabajo más ágilmente. Por ejemplo, puede dividirse:

- Coste del impacto que tiene el riesgo sobre la organización en el caso de que la amenaza explotará la vulnerabilidad del activo, es decir, en el supuesto que se materialice el riesgo.
- Coste potencial de la no implementación del control. La organización debe aplicar la regla de oro analizando: Riesgo vs. Control vs. Coste

PROCESO CONTINUO

Es necesario tener en cuenta que **la seguridad no es una meta que se pueda alcanzar**, por la propia naturaleza del contexto que se maneja ocurren una serie de acciones que imposibilita alcanzar esta meta. Día a día se descubren nuevas vulnerabilidades, las amenazas siguen evolucionando y los puntos débiles en el sistema cambian, convirtiéndose en nuevos puntos de ataque. También existe un **factor psicológico** ya que el personal se puede relajar o encontrar formas de rodear las medidas de seguridad por temas de usabilidad.

Y no solo es un proceso, es también una actitud. Cualquier confianza es limitada, ya que se debe asumir que el atacante es al menos tan inteligente e incluso más motivado que los defensores. Se debe asumir que los puntos más débiles son los objetivos más probables y que la seguridad se puede ganar o perder incrementalmente a través de pequeñas acciones o inacciones.

1.2.1 Estándares y normativas de seguridad en la industria

Varias organizaciones han desarrollado sus propias aproximaciones hacia la gestión de la seguridad, control de objetivos de la seguridad, gestión de procesos y desarrollo empresarial. Algunas de las **regulaciones** son:

- Programa de desarrollo seguro:
  - ISO/IEC 27000 series, Normas internacionales sobre cómo desarrollar y mantener un SGSI desarrollado por ISO y IEC
- Desarrollo de Arquitectura Empresarial:
  - Zachman Framework, Modelo para el desarrollo de arquitecturas empresariales desarrollado por John Zachman
  - TOGAF, Modelo y metodología para el desarrollo de arquitecturas empresariales desarrolladas por The Open Group
  - DoDAF, Framework de arquitectura del Departamento de Defensa de los Estados Unidos que garantiza la interoperabilidad de los sistemas para cumplir los objetivos de la misión militar
  - MODAF, Framework de arquitectura utilizado principalmente en las misiones de apoyo militar desarrollado por el Ministerio de Defensa británico
  - SABSA model Modelo y metodología para el desarrollo de arquitecturas empresariales de seguridad de la información
- Desarrollo de controles de seguridad:
  - COBIT 5, Un marco de negocios para permitir a las empresas de TI gestionar y gobernar, fue desarrollado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA)
  - NIST SP 800-53, Conjunto de controles para proteger los sistemas federales estadounidenses desarrollados por el Instituto Nacional de Estándares y Tecnología (NIST)
  - COSO Internal Control—Integrated Framework, Conjunto de controles corporativos internos para ayudar a reducir el riesgo de fraude financiero desarrollado por el Comité de Organizaciones Patrocinadoras (COSO) de la Treadway Commission.

- Desarrollo de la Gestión de Procesos:
    - ITIL, es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información.
    - Six Sigmam Estrategia de gestión empresarial que puede utilizarse para llevar a cabo la mejora de procesos
    - Capability Maturity Model Integration (CMMI) Desarrollo organizacional para la mejora de procesos desarrollado por Carnegie Mellon University
- Controlar acceso a los sistemas financieros: legislación Sarbanes-Oxley.
- Proteger información de tarjetas de crédito: PCI DSS standards.
- Proteger infraestructura crítica: NERC CIP, ANSSI standard, FDA 510(k).
- También existen numerosas regulaciones en OT como puede ser:
    - ISA 99
    - IEEE pc37.240
    - Safety Integrity Level (SIL)
    - Critical Infrastructure Protection (CIP)
    - Critical Infrastructure Security (CIS)
    - Current Good Manufacturing Practices (CGMP)
    - Emissions control with Environment Protection
    - Agency (EPA) and Marine Pollution (MARPOL)
    - Facilities Standards with Energy Performance of Building Directive (EPBD)
    - Motor Efficiency with Minimum Energy Performance Standards (MEPS)

1.2.2 Normativas Europeas

Comunicación de la Comisión al Consejo y al Parlamento Europeo, del 20 de octubre de 2004, sobre Protección de infraestructuras críticas en la lucha contra el terrorismo

Dicha Comunicación describe las acciones que la Comisión ha venido adoptando hasta su fecha de emisión de cara a proteger adecuadamente las Infraestructuras Críticas (en adelante IC).

En su apartado 3.1 se define a las IC como:

"Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros".

Además se ha creado una red de información sobre alertas en materia de IC denominada CIWIN (Critical Infrastructure Warning Information Network) cuyo fin es agrupar a los especialistas en la materia de los Estados miembros de la Unión Europea.

Comunicación de la Comisión, de 12 de diciembre de 2006, sobre un Programa Europeo para la Protección de Infraestructuras Críticas (PEPIC)

El objetivo general del PEPIC, según se indica en su apartado 2.1., es el de mejorar la protección de las IC de la Unión Europea mediante la creación de un marco común en el seno de la misma relativo a su protección.

1.2.3 Normativa Española

Ley 8/2011, de 28 de abril, de Medidas para la Protección de las Infraestructuras Críticas

La Ley de Protección de Infraestructuras Críticas (en adelante PIC) tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de IC

Asimismo, en virtud de la Ley PIC se crea el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC)

Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC)

El PNPIC es el instrumento de programación del Estado elaborado por la Secretaría de Estado de Seguridad y dirigido a mantener seguras las infraestructuras españolas que proporcionan los servicios esenciales a la sociedad.

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad

Su objeto es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

1.3 AMENAZAS EN LOS ENTORNOS INDUSTRIALES

Una **amenaza** es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema. Esto incluye tanto daños a equipamiento a nivel físico como a su funcionalidad e información.

Las amenazas de los sistemas de control y automatización pueden ser **de tipo intencionado o no intencionado**. Según Security Incidents Organization existe una tendencia incremental de las amenazas de origen intencionado, aun siendo la mayoría, de hasta el 80%, de origen no intencionado.

Además también se pueden diferenciar las **amenazas oportunistas y dirigidas**. Las amenazas oportunistas son ataques automatizados aprovechando vulnerabilidades conocidas. En este caso es fácil identificar que alguien ha sido atacado. Por otra parte las amenazas dirigidas se dividen en:

- **Puntuales:** Con pocos medios y menor probabilidad de éxito. Fáciles de detectar
- **Persistentes y Avanzadas (Advanced Persistent Threat):** Atacantes motivados y con grandes habilidades y conocimientos. Difíciles de detectar.

- **Advanced:** Ejecutado por grupo con un alto conocimiento y con muchos recursos (herramientas).
- **Persistent:** Es un ataque lento para evitar la detección y enfocado a un objetivo.
- **Threat:** Está financiado, coordinado y con una serie de metas objetivos.

1.3.1 Amenazas no intencionadas

Las amenazas no intencionadas incluyen todas aquellas que **no afectan específicamente a los sistemas de control y automatización**, pero que, por diversos motivos, pueden suponer un peligro para estos sistemas. Habitualmente, las amenazas no intencionadas están relacionadas con fenómenos que no podemos controlar.

Las amenazas no intencionadas se clasifican en los siguientes grupos.

ILUSTRACIÓN 12: AMENAZAS EN ENTORNOS INDUSTRIALES NO INTENCIONADAS

Lo fallos de "*Safety*" son problemas que pueden tener los propios sistemas de protección, el resto de grupos derivan de la propia naturaleza del entorno o individuo.

1.3.2 Amenazas intencionadas

Las amenazas intencionadas incluyen todas aquellas fuentes de problemas que **van dirigidos expresamente contra los sistemas de control**, generalmente las amenazas intencionadas tienen un origen humano. En la siguiente figura se listan las principales motivaciones.

ILUSTRACIÓN 13: MOTIVACIONES DE AMENAZAS INTENCIONADAS

Los atacantes generarán una serie de amenazas a través de **distintos vectores de ataque**[11]. Los ataques más usuales y representativos son:

- Robo.
- Destrucción física.
- Malware: Programa maliciosos diseñados con múltiples propósitos.
- Manipulación de comunicaciones.
- Escalado de privilegios: Obtención de manera ilícita un recurso no disponible para un usuario o aplicación.
- Inyección de código: Explotación de las debilidades de aplicaciones para obtención de información a través de entradas destinadas a otra función.
- Denegación de servicio.
- Spoofing: Suplantación de identidad con intención maliciosa.
- Repetición: Inyección de tráfico antiguo alterado.
- Ingeniería social: Trata de obtener información a través de la manipulación de usuarios legítimos.
- Phising: Un ataque phising suplanta una persona o empresa de confianza a través de una comunicación oficial electrónica.
- Spam.

[11] Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

1.4 TENDENCIAS

"Safety and security: Safety and security are both critical to the success of smart manufacturing systems. It is important to ensure that production facilities and the products themselves do not pose a danger either to people or to the environment. At the same time, both production facilities and products and in particular the data and information they contain – need to be protected against misuse and unauthorised access." [12]

El desarrollo de determinadas tecnologías y ciertas tendencias permiten vislumbrar importantes cambios que se van a producir en la industria a corto y medio plazo y que está dando lugar a lo que se empieza a conocer como "Industria 4.0", una revolución industrial que aún no se ha producido.

Los conceptos de safety & security[13] son dos aspectos clave tanto desde el punto de vista de los procesos industriales como de los productos producidos. Por un lado, **no deben suponer peligro para las personas ni para el medio ambiente (safety)** mientras que, por otro lado, las instalaciones y los productos de producción -y en particular los datos y conocimientos técnicos que contienen- deben protegerse contra el **uso indebido y el acceso no autorizado (security)**. Las cuestiones asociadas a safety han sido tradicionalmente un aspecto muy importante en el diseño de las instalaciones de fabricación, en los procesos productivos y en los productos, estando regulado habitualmente por un conjunto de normas y estándares que rigen su diseño y funcionamiento.

En los **sistemas automáticos y robóticos** de producción la seguridad es un aspecto fundamental. Tradicionalmente se garantiza la seguridad mediante barreras de seguridad y sensores que separan a las personas y los sistemas automáticos. La introducción de los sistemas de automatización avanzados y de robótica colaborativa requieren que se eviten esas barreras y que los operarios y las máquinas compartan el espacio de producción sin riesgo.

En los últimos años están surgiendo en el mercado nuevos sistemas de automatización y robótica colaborativa, que introducen elementos de seguridad que reducen los riesgos mediante la introducción de sensores e incluyendo inteligencia en los sistemas automáticos para actuar de un modo seguro. Sin embargo, aún hay grandes retos pendientes para la implantación de sistemas automáticos colaborativos seguros en los que las personas y los sistemas automáticos se reparten las actividades productivas.

En contraste con el concepto de safety, security ha recibido menos atención por parte de la industria manufacturera porque los riesgos potenciales eran relativamente reducidos. La implantación de la Industria 4.0 y del **Internet de las Cosas Industria (IIoT)** van a exponer muchos sistemas e información crítica de la empresa a Internet, haciendo estos más vulnerables a un uso indebido o ilegítimo. La implantación de la Industria 4.0 y la interconexión de los diferentes elementos de una Smart Factory van a generar importantes riesgos en cuanto a seguridad, con nuevas vulnerabilidades que será necesario tratar para que tanto las instalaciones como los productos - y los datos y la información que contienen – sean protegidos contra un uso fraudulento o no autorizado.

[12] Recommendations for implementing the strategic initiative INDUSTRIE 4.0, 2013,

acatech – National Academy of Science and Engineering.

[13] Se utilizan los términos "safety" y "security" en inglés para distinguir entre las dos concepciones de seguridad.

La digitalización de la fábrica y la conectividad lleva aparejada una preocupación de las empresas por la ciberseguridad como una de las barreras de adopción de la Industria 4.0. Las empresas deberán identificar y gestionar los riesgos que suponen la introducción de las tecnologías de la Industria 4.0, ya que sus máquinas, sus procesos productivos, sus fábricas y sus datos estarán más expuestos a usos malintencionados. **La gestión de la seguridad será un elemento clave en la implantación de soluciones de Industria 4.0**, con los siguientes **objetivos de protección**:

- Disponibilidad e integridad
- Seguridad operacional
- Protección del know-how
- Protección de Datos

Internet de las Cosas es un nuevo paradigma en el que los objetos físicos se integran perfectamente en las redes de información y se convierten en participantes activos dentro de campos tan variados como procesos de negocio o el día a día de una persona. Diversos tipos de servicios serían capaces de interaccionar con estos objetos inteligentes, consultar su estado y cualquier tipo de información asociada, teniendo en cuenta la seguridad y privacidad necesarias para llevar a cabo estas operaciones

Asociado al desarrollo de IoT se plantea la necesidad de desarrollar **nuevas herramientas de seguridad TI y ciberseguridad** para la protección de datos y servicios en sistemas (digitales) contra el uso indebido, como por ejemplo el acceso no autorizado, modificación o destrucción de información. Dependiendo del sistema tecnológico en cuestión y de los datos y servicios que incorpore, la seguridad proporciona la base para la privacidad de la información, es decir, la protección de las personas contra las infracciones de sus derechos de datos personales. También permite la protección del know-how, es decir, la protección de los derechos de propiedad intelectual. Los objetivos de las medidas de seguridad son aumentar:

- La **confidencialidad:** restricción del acceso a datos y servicios a máquinas específicas/usuarios humanos.
- La **integridad**: exactitud / exhaustividad de los datos y correcto funcionamiento de los servicios.
- La **disponibilidad**: medida de la capacidad de un sistema para realizar una función en un tiempo determinado.

En el documento "Recommendations for implementing the strategic initiative INDUSTRIE 4.0"[14] de **Acatech** se establecen los siguientes aspectos a considerar son:

- Métodos de medición de los potenciales y riesgos de las amenazas, incluido un análisis coste/beneficio de las medidas de seguridad
- Protección de interfaces en las relaciones externas e internas
- Protección de los sistemas de comunicación dentro de la instalación
- Impacto de las lagunas de seguridad en los riesgos de seguridad operativa
- Relación con requisitos legales, como por ejemplo protección de datos
- Seguridad por diseño (Security by design)

[14] Recommendations for implementing the strategic initiative INDUSTRIE 4.0, 2013,

acatech – National Academy of Science and Engineering.

- Viabilidad a largo plazo de las soluciones de seguridad
- Detección y análisis de ataques

Aparte de los retos técnicos, el éxito de la implantación de soluciones de safety & security tendrán que tener en cuenta **aspectos económicos, psicológicos y educativos**. Para lograr un alto nivel de aceptación, las soluciones deben ser fáciles de usar, disponer de herramientas para ayudar a los desarrolladores y proporcionar métodos eficientes de evaluación de la seguridad.

Bajo el paraguas de IoT se encuentran un conjunto de tecnologías relacionadas y habilitadoras, y estándares. Existen diversas entidades que están trabajando en la definición de una arquitectura de referencia para IoT, en la que se definan los estándares que dan soporte a IoT y las diferentes capas que conforman la arquitectura. En el apartado de estandarización se analizarán con más detalles la situación actual.

En la arquitectura de referencia definida por la Unión Internacional de las Telecomunicaciones en la recomendación ITU-T Y.2060[15] se establecen cuatro capas: dispositivos, red, soporte al servicio y soporte a la aplicación, y aplicación. Además de estas cuatro capas, consta de capacidades de gestión y de seguridad relacionadas con ellas. La capa de **capacidades de seguridad** se divide en:

- Capacidades de gestión de seguridad **genéricas**:
  - En la capa de aplicación: autorización, autenticación, confidencialidad de datos de aplicación y protección de la integridad, protección de la privacidad, auditorías de seguridad y antivirus.
  - En la capa de red: autorización, autentificación, confidencialidad de datos de señalización y de datos de uso, y protección de la integridad de señalización.
  - En la capa de dispositivo: autenticación, autorización, validación de la integridad del dispositivo, control de acceso, confidencialidad de datos y protección de la integridad.

- Capacidades de gestión de seguridad **específicas** dependientes de las particularidades y requisitos de la aplicación.

[15] Recomendación ITU-T Y.2060, ITU, 2012, https://www.itu.int/rec/T-REC-Y.2060-201206-I/es

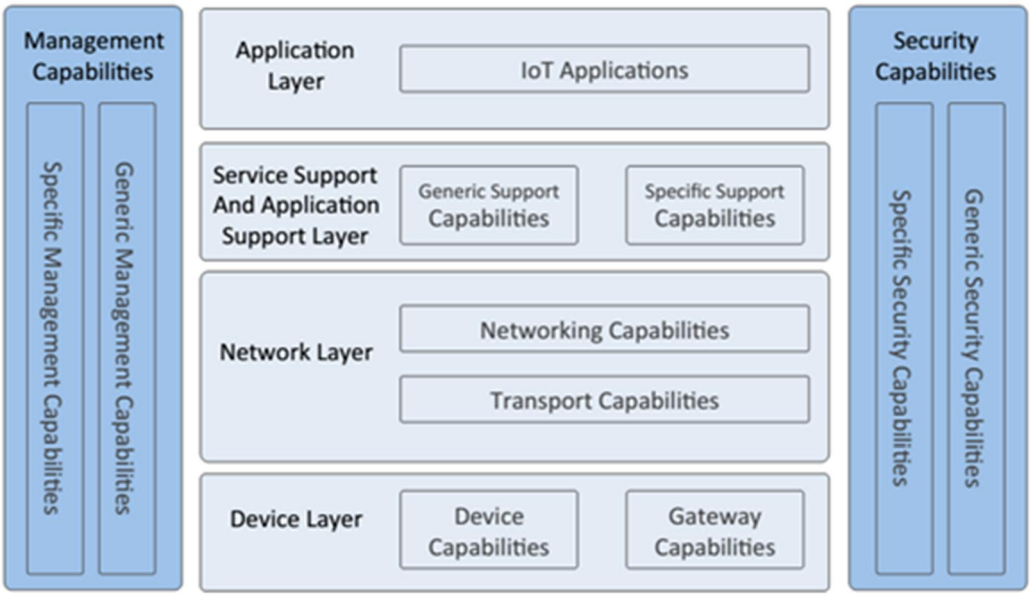


ILUSTRACIÓN 14: MODELO DE REFERENCIA ITU-T Y.2060. FUENTE IERC

El **cloud computing** representa un cambio importante en cómo pueden las empresas procesar la información y gestionar las áreas TIC; apreciándose que con la gestión TIC tradicional las empresas realizan cuantiosas inversiones en recursos, incluyendo hardware, software, centros de procesamiento de datos, redes, personal, seguridad, etc.; mientras que con los modelos de soluciones en la nube se elimina la necesidad de grandes inversiones y costes fijos, transformando a los proveedores en empresas de servicios que ofrecen de forma flexible e instantánea la capacidad de computación bajo demanda.

El uso de la computación en la nube tiene varias implicaciones a nivel de seguridad y de carácter legal debido a la localización de los servidores en **países que no tienen por qué ser los de origen de los datos**. Otra de las principales preocupaciones en este sentido de los usuarios del modelo de computación en la nube es la posible coexistencia en la nube de datos críticos con otros de competidores y la posible pérdida sobre el control de los mismos. Múltiples proyectos se encargan en la actualidad de buscar medidas para dar una solución a esta problemática.

Teniendo en cuenta que Industrie 4.0 incrementará la cooperación en toda la cadena de valor, será necesario que las distintas entidades tengan un elevado grado de **confianza mutua** (seguridad y confianza) y que proporcionen evidencia de sus competencias de seguridad. Tanto en este aspecto como en general en IoT, la verificación segura de la identidad es de crucial importancia para la Industria 4.0, tanto a nivel de identificación de usuarios, máquinas, sistemas software...

La siguiente tabla muestra algunas de las **amenazas y vulnerabilidades** asociadas al desarrollo de IoT y los sistemas ciberfísicos.

Base/tendencia tecnológica	Amenazas / Vulnerabilidades	Retos	Tratamiento/reto seguridad
Sistemas ciberfísicos (CPS)	Ciberataques en los sistemas CPS (espionaje industrial inclusive) Malware (desconocido) en la industria. Denegación de servicio interno.	Ciberseguridad en la fábrica del futuro. Industria 4.0 y ciberseguridad. Interacción segura en SoS (sistemas de sistemas)	Segmentación de red adecuada. Acceso restringido en la operación con sistemas físicos. Virtualización custodiada. Detección de malware desconocido. Detección de comportamientos anómalos e inciertos. Bloqueo instantáneo del tráfico de red. Criptografía de baja latencia
Internet de las cosas	Ataques Tampering Criptografía vulnerable	Privacidad Ingeniería inversa Conocimiento de HW por integradores e incluso fabricantes Tiempo real	Elementos fortificados. Elementos seguros (HSM). Uso de claves preinstaladas de forma segura. Conexión segura con terceras partes. Aislamiento medio. Cifrado en tiempo real (acelerado por hardware y controlado por software).
Internet de los servicios	Denegación de servicio externo o inter-organizacional Acceso no restringido por parte del personal.	BYOD Decisión en los SLAs	SLA correctos y dinámicos. Requisitos de ciberseguridad argumentados. Conexión asegurada. Medición de efectos en cascada y plan de contingencia. Control de acceso y sistema de autorización unívoco y dirigido.

ILUSTRACIÓN 15: ALGUNAS DE LAS AMENAZAS, VULNERABILIDADES Y POSIBLES RETOS/SALVAGUARDAS EN TORNO A LA CIBERSEGURIDAD[16]

[16] La Ciberseguiridad en la Industria 4.0 - Incibe

2. PRINCIPALES TECNOLOGÍAS DE LA INDUSTRIA

En este apartado se explicará las **distintas soluciones existentes**, desde que tipos de controles a aplicar en procesos de *Safety* y *Security* así como que productos son aplicables a cada una de las ramas y arquitecturas de securización.

2.1 TIPOS DE CONTROLES

La terminología de seguridad usada en la industria (vulnerabilidad, riesgo, amenaza, control) y los objetivos globales (disponibilidad, integridad, confidencialidad) son componentes fundamentales que deben ser entendidos si la seguridad va a tener lugar en la organización. El siguiente problema fundamental que vamos a abordar son los **tipos de control** que se pueden implementar y su **funcionalidad asociada**.

Es necesario ejecutar ciertos controles para proporcionar **defensa en profundidad.** La defensa en profundidad coordina el uso de múltiples controles para un enfoque en capas. Un sistema de defensa de múltiples capas minimiza la probabilidad de penetración exitosa ya que un atacante tendría que pasar por varios mecanismos de protección antes de que accediera a los activos críticos.

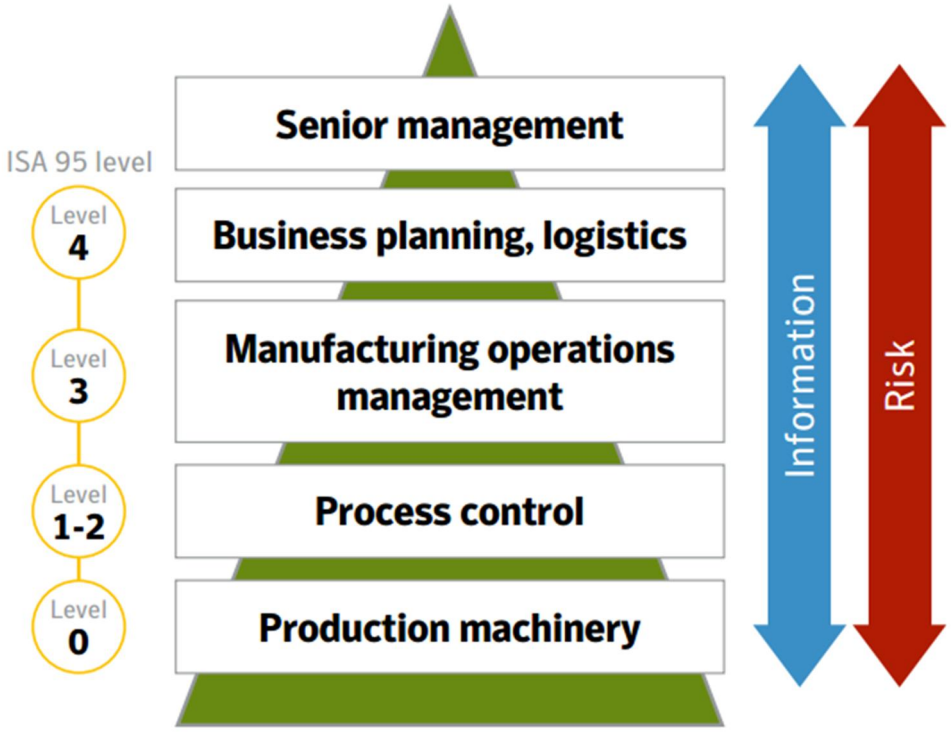


ILUSTRACIÓN 16: FLUJO DE LA INFORMACIÓN Y RIESGO A TRAVÉS DE LA INDUSTRIA 4.0[17]

[17] Smarter Security For Manufacturing in the Industry 4.0 ERA - Sysmantec

Por ejemplo, la empresa A puede tener los siguientes **controles físicos** funcionando en un modelo de capas:

- Valla
- Puertas exteriores cerradas
- Circuito cerrado de televisión
- Guardia de seguridad
- Puertas internas
- Sala de servidores securizadas

Los **controles técnicos** que generalmente se despliegan para proporcionar este tipo de enfoque en capas son:

- Cortafuegos
- Sistema de detección de intrusos
- Sistemas de prevención de intrusiones
- Antimalware
- Control de acceso
- Cifrado

Los controles que se implementan deben **mapear las amenazas a** las que se enfrenta la empresa, además, el número de capas debe correlacionarse con la sensibilidad del activo. Una regla comúnmente aceptada es, según más sensible sean los activos, más capas de protección deben ser puestas.

Una clasificación de las **diferentes categorías de controles** que se pueden utilizar son: **administrativas, técnicas y físicas**. Pero, para entender qué hacen realmente estos controles por la empresa es necesario entender las diferentes funcionalidades que cada tipo de control puede proporcionar para proteger nuestros entornos.

Teniendo una mejor comprensión de las diferentes funcionalidades de control, se podrá tomar decisiones más informadas sobre cuáles son los mejores controles para utilizar en situaciones específicas. Las seis **diferentes funcionalidades de control** son:

- **Preventivo:** Destinado a evitar que se produzca un incidente.
- **Detección:** Ayuda a identificar las actividades de un incidente y potenciales intrusos.
- **Correctivo:** Arreglar componentes o sistemas después de que se ha producido un incidente.
- **Disuasorio:** Para disuadir a un posible atacante.
- **Recuperación:** Devolver al entorno las operaciones normales.
- **Compensación:** Controles que proporcionan una medida alternativa de control.

En una estructura de seguridad de un entorno, es más productivo usar un modelo preventivo y luego usar mecanismos detectores, correctivos y de recuperación para apoyar este modelo.

Básicamente se quiere detener cualquier problema antes de que comience, sin embargo, no es posible prevenirlo todo; Por lo tanto lo que no se puede evitar se debe ser capaz de detectar rápidamente, reaccionar y combatir los problemas que se encuentren.

Es por eso que los **controles preventivos y de detección** siempre deben ser implementados juntos y deben complementarse.

Ampliando este concepto: lo que no se puede evitar, se debe ser capaz de detectar, y si se detecta algo significa que no se fue capaz de prevenirlo, por lo tanto se debe tomar medidas correctivas para asegurarse de que en un futuro se podrá impedir. Por eso la prevención, detección y corrección funcionan en conjunto.

Los tipos de control **administrativos, físicos y técnicos** son de naturaleza preventiva. Es importante conocerlos y entenderlos para cuando se desarrolla un programa de seguridad para toda la empresa.

La siguiente tabla muestra cómo estos tipos de mecanismos de control realizan diferentes funciones de seguridad.

	PREVENCIÓN	DETECCIÓN	CORRECCIÓN	DISUASIÓN	RECUPERACIÓN	COMPENSACIÓN
Tipo físico						
Vallas				x		
Cerraduras	x					
Sistema de credenciales	x					
Guardia de seguridad	x					
Sistema de biometría	x					
Doble puerta de seguridad	x					
Alumbrado				x		
Detectores de movimiento		x				
Circuito Cerrado de TV		x				
Instalaciones externas					x	
Tipo administrativo						
Políticas de Seguridad	x					

Monitorización y supervisión		x			
Separación de obligaciones	x				
Rotación de trabajos		x			
Clasificación de la información	x				
Procedimientos personales	x				
Investigaciones		x			
Testing	x				
Conciencia de seguridad	x				
Tipo Técnico					
ACLs	x				
Encriptación	x				
Logs de auditoría		x			
IDS		x			
Antivirus	x				
Imagenes de servidor			x		
Tarjetas inteligentes	x				
Sistemas de devolución de llamada telefónica	x				
Backups de datos				x	

TABLA 1. FUNCIONES DE SEGURIDAD QUE REALIZAN LOS DISTINTOS MECANISMOS DE CONTROL

2.2 GESTIÓN DE RIESGOS

El primer paso para estudiar la seguridad de un sistema es analizar sus riesgos. Las empresas deben cumplir la legislación al respecto, pero más allá de eso, la seguridad está al servicio del negocio.

La seguridad no proporcionará dinero a la empresa, pero se asegura de que no lo pierda. El **Retorno de Inversión de Seguridad** representa lo que dejo de perder por invertir en seguridad.

Para ello es imprescindible conocer el riesgo sobre los activos y alcanzar una estimación económica de los mismos. Esto suele ser especialmente complicado en seguridad por dos motivos:

1. Difícil **valorar los activos**. ¿Cuánto vale nuestra base de datos de clientes?
2. Difícil **estimar la probabilidad de una exposición**.

El **análisis de riesgos** debe ser el primer paso. Cualquier otro orden provocará que invirtamos dinero en proteger activos que no tienen por qué ser nuestra prioridad. Normalmente la seguridad se consideró un trabajo de los informáticos, los controles no son siempre técnicos, muchas veces son más baratos y eficaces los administrativos. El responsable de la información y de los servicios (activos esenciales) no es seguridad ni sistemas, es negocio. Ellos son los que deben determinar el valor de los mismos. Además el riesgo se mitiga o se transfiere, pero nunca se elimina.

El **riesgo residual** debe asumirse y conocerse. Otra posibilidad es transmitirlo a través de pólizas de seguros, pero sólo se transmite una protección económica, no una protección del activo (un seguro de vida no asume el riesgo de muerte, lo compensa).

El análisis y gestión del riesgo es un tema ampliamente discutido en la literatura. Metodológicamente existen varias ideas generales a tener en cuenta. Existen dos maneras de calcular el riesgo, el análisis cualitativo y el cuantitativo.

Es necesario usar el **análisis cualitativo** cuando no es posible establecer de manera adecuada el valor de un activo. Este análisis suele ser el habitual en seguridad al ser un dominio incierto.

Los análisis se basan en la **probabilidad e impacto (cualitativo)** de que se produzca una exposición. Este impacto se define como cualitativo al no tener una relación directa con el coste del riesgo. Por ejemplo, en el caso de la banca un robo online de 100€ tiene un impacto mucho mayor en la imagen corporativa.

Es necesario un análisis para clasificar los riesgos y establecer prioridades en su tratamiento como se muestra en la siguiente figura.

	Impacto				
Probabilidad	Insignificante (1)	Menor (2)	Moderado (3)	Alto (4)	Catastrófico (5)
Muy probable	M	A	E	E	E
Probable	M	A	A	E	E
Posible	B	M	A	E	E
Improbable	B	B	M	A	E
Muy improbable	B	B	M	A	A

HOJA DE CÁLCULO INCIBE PARA LA GESTIÓN DE RIESGOS

2.3 SECURIZACIÓN DE ENTORNOS CRÍTICOS

2.3.1 Pentesting en entornos seguros

Según la wikipedia, **pentesting o prueba de penetración** es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos.

La finalidad de un pentesting es la mejora de seguridad del entorno, ayudar a determinar si un sistema es vulnerable a los ataques, si las defensas (si las hay) son suficientes y no fueron vencidas

2.3.2 Defensa en profundidad

Paul Brooke define la defensa en profundidad como:

"La práctica de la defensa en capas para proporcionar una protección añadida. La defensa en profundidad aumenta la seguridad al elevar el costo de un ataque. De esta forma se hace que sea más difícil los ataques gracias a las múltiples barreras entre un atacante y los recursos de información críticos para el negocio. Estas múltiples capas previenen los ataques directos contra los sistemas importantes y evita el fácil reconocimiento de las redes. Además, una estrategia de defensa en profundidad ofrece espacios naturales para la aplicación de las tecnologías de detección de intrusos. Idealmente, las medidas de defensa en profundidad aumentan el tiempo para detectar y responder a una violación, lo que reduce su impacto"

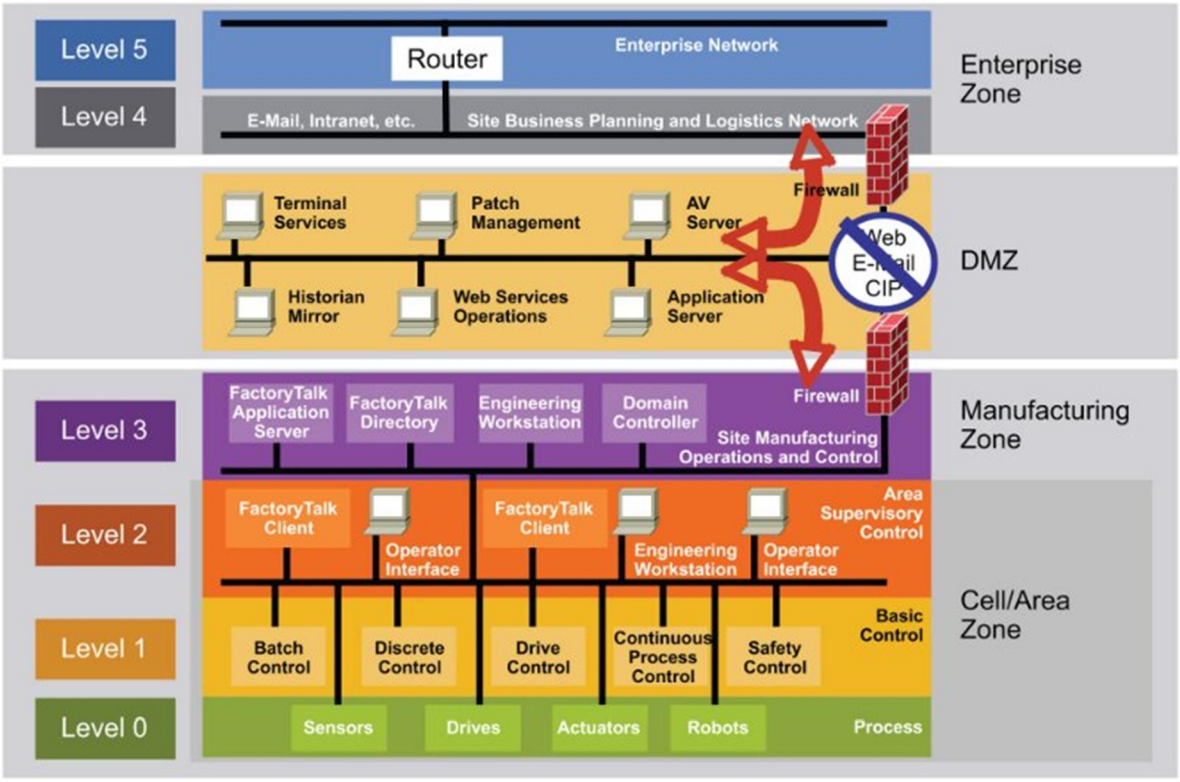


ILUSTRACIÓN 17: CAPAS EN LA INDUSTRIA[18]

[18] Industrial Demilitarized Zone Design Principles - Rockwell Automation

Los ataques efectuados a esta división por niveles no son homogéneos, cada uno de los niveles recibe unos ataques distintos y en distintas cantidades como se puede observar en el siguiente diagrama.

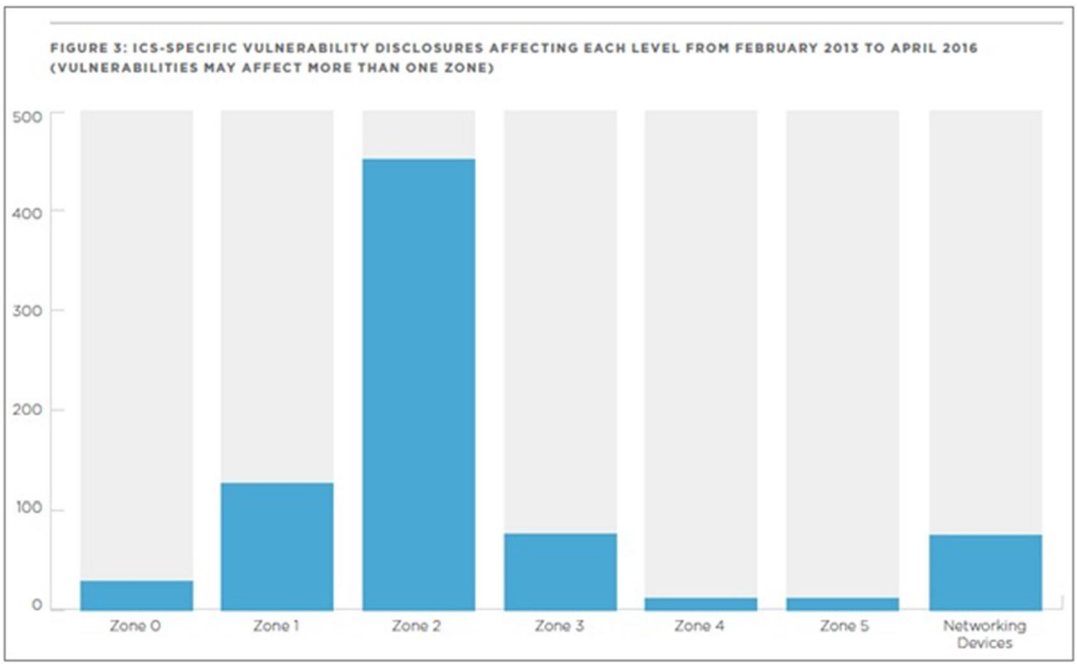


ILUSTRACIÓN 18: DISTRIBUCIÓN DE LOS ATAQUES SEGÚN LA ZONA[19]

Para alcanzar los niveles deseados de **cibersecurización** en industria nos podemos apalancar en esta estructura, dividiendo la seguridad en los siguientes puntos:

- Seguridad del software.
- Seguridad del hardware.
- Seguridad de la red.
- Seguridad física.

En diagrama siguiente se muestra cómo aplicar esta protección en una securización por capas:

[19] FireEye 2016 ICS Vulnerabilities Trend Report: Missed Warnings, Exposed Industrial Environments

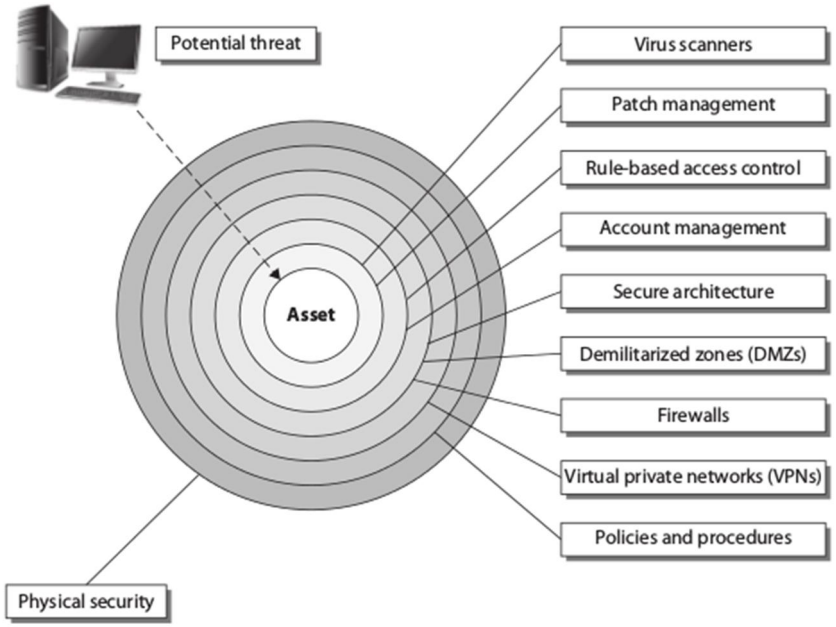


ILUSTRACIÓN 19: ESCENARIO GENERAL DE SECURIZACIÓN POR CAPAS DE UN ACTIVO

2.3.3 Conciencia de seguridad

Como suele ocurrir, el mayor **punto débil del proceso** no está en los sistemas, sino en las personas. Esto suele ocurrir por muchos motivos, generalmente por una pobre cualificación o actualización de los empleados.

Dentro de los programas de formación de seguridad, algunos de los **puntos clave para empleados** son:

- Concienciación de la política de seguridad de la organización.
- Impacto del acceso no autorizado.
- Conocimiento de los requisitos de seguridad para diferentes entornos.
- Buenas prácticas en correo electrónico, navegación, dispositivos móviles etc.
- Cómo informar de un posible incidente de seguridad y a quién.
- Seguridad física.
- Shoulder Surfing (mirar por encima del hombro).
- Dumpster Diving (búsqueda en los contenedores).

2.4 MEDIDAS DE DETECCIÓN

2.4.1 Auditorías de seguridad

Es importante realizar auditorías de seguridad continuada en el tiempo para analizar y evaluar los niveles de seguridad. Estas deben ser:

- **Auditorías técnicas.** Es aconsejable realizar test de intrusión internos y externos, así como test de vulnerabilidades y análisis de la red. Con los resultados obtenidos se puede generar un documento que refleje el nivel de seguridad del sistema, así como un plan de acción para corregir, mitigar o asumir aquellos fallos que se hayan detectado.
- **Auditorías físicas.** En función del alcance y tamaño de la red, se recomienda realizar inspecciones físicas en un conjunto aleatorio y representativo de instalaciones, evaluando la seguridad física existente y contrastándola con la requerida en la política de seguridad física y ambiental de la compañía.

2.4.2 Inventariado, monitorización y control de los sistemas

Es importante generar y mantener actualizado un inventario de equipos y sistemas de la red de monitorización y control, en el que para cada activo se recoja, al menos, la siguiente información: identificador, situación geográfica, finalidad, criticidad, responsable y gestor. Este inventario permite, entre otras cosas, la detección de equipos o elementos no autorizados en la red.

2.4.3 Trazas de auditoría

Siempre que sea posible, se recomienda activar el uso de registros de auditoría. Con ello, será posible registrar los accesos fallidos, ya sea de los propios usuarios, de sistema o de aplicación.

2.5 EJEMPLOS DE PRODUCTOS

Dentro de todos los tipos de controles, existen muchas innovaciones y mejoras. En el siguiente listado se presentan **nuevos productos o productos consolidados** a modo de ejemplo del tipo físico y técnico, ya que son los más propensos a innovación tecnológica. Además existen decenas de productos por cada tema, por lo que se simplificará la muestra.

2.5.1 Tipo Físico

CERRADURAS

REMOTELOCK

RemoteLock ACS es un sistema de gestión de acceso basado en la nube que integra controladores externos de puerta con cerraduras conectadas vía Wi-Fi. Monitoriza la actividad de los usuarios, modificar privilegios y mantiene logs en tiempo real visibles desde cualquier ordenador.

AUGUST

El kit completo consta de Doorbell Cam (Una cámara y micrófono controlados por wifi para ver y hablar con el visitante) + Smart Lock 2nd Generation (la propia cerradura) + Smart Keypad (para el acceso basado en pin) + Connect (hub para conectar todo el sistema a través de la wifi). Todo esto permite la monitorización y activación a través de internet de la cerradura.

SISTEMA DE CREDENCIALES

ALPHACARD

Los sistemas de identificación del empleado ayudan a agilizar las operaciones de la empresa, identificando fácilmente a los trabajadores. AlphaCard proporciona sistemas completos que incluyen una impresora de tarjetas de ID, el software necesario (diseño y bases de datos), y suministros para la impresión.

CIC SMARTBADGE

Es un dispositivo compacto y alimentado por baterías con las siguientes características:

- Duración de la batería de hasta 4 semanas
- 2.4G / 5GHz de doble banda de conexiones WiFi
- Ubicación en el interior
- Función de voz PTT
- Función NFC integrada
- Sensores integrados de temperatura, movimiento
- Pantalla OLED y mensajería

SISTEMAS DE BIOMETRÍA

TASCENT

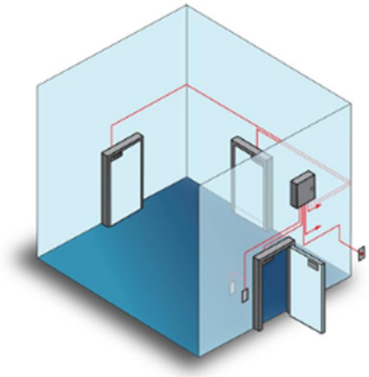
Tascent InSight One es un sistema de reconocimiento basado en el Iris. captura ambos Iris y la cara a una distancia de 0.5m o 1m. Se usa para la identificación y acceso. Tascent M6 se integra con el iphone 6 proveyendo reconocimiento de huella dactilar, voz, cara e Iris.

NEC

Desde hace 40 años, NEC provee soluciones biométricas. Sus tecnologías de identificación se basan en huella dactilar, palma, y reconocimiento de cara. Para las infraestructuras críticas tiene soluciones concretas de analizador de comportamiento (video analytics) y buscador de metadatos a través de los videos.

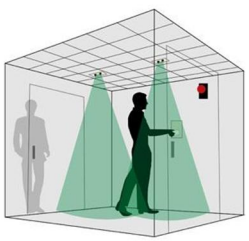
DOBLE PUERTA DE SEGURIDAD (MANTRAP DOORS)

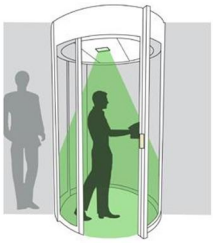
SDC



SDC se especializa en la manufactura de la seguridad de controles de accesos y puertas de seguridad, sistemas de bloqueo y sistemas de comunicación de baños. Utiliza sistemas para la lectura de proximidad, lectores de tarjeta rfid y teclados de acceso.

BOON EDAM

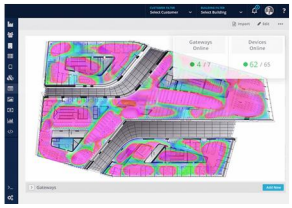




Boon Edam provee portales todo-en-uno para evitar el tener que construir vestíbulos de seguridad de paso. Esto simplifica el acceso a las personas y el uso autónomo. Además son resistente a las balas, proveen métricas de acceso y tienen detectores de metal para una máxima seguridad.

ALUMBRADO

GOOEE



Gooee propone un ecosistema completo para la gestión de iluminación en cualquier entorno. Una de sus premisas es el uso de algoritmos para optimizar los ajustes de luz a lo largo del día basado en la presencia, niveles de luz ambiente y actividad del área.

HONEYWELL

Honeywell es uno de los mayores fabricantes de productos de ingeniería. Está preparado para grandes despliegues e integra un sensor fotovoltaico para balancear la luz natural y artificial y un módulo para usuarios para el oscurecimiento/selección de escena.

DETECTORES DE MOVIMIENTO

BOSCH

Bosh provee distintos detectores y accesorios para la detección de intrusos y la reducción de falsas alarmas como puede ser los Sensores infrarrojos pasivos (PIR), sensores de microondas, beams fotoeléctricos, sísmicos, rotura de cristales y sensores magnéticos empotrados.

XTRALIS

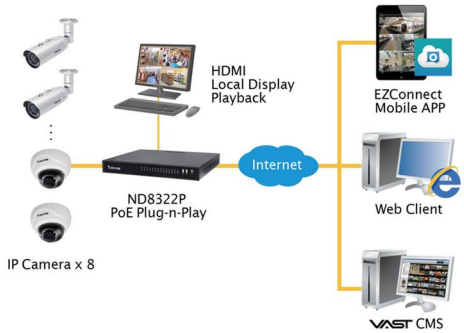
Xtralis tiene diferentes soluciones de detección de movimiento para la seguridad perimetral, como por ejemplo ADPRO PRO (PIR detector) o E-PIRs. Además sus soluciones para la detección de movimiento se completan con cámaras de seguridad y audiometría

CIRCUITO CERRADO DE TV - VIDEOVIGILANCIA IP

MOXA

La solución de video vigilancia sobre IP es la renovación de los clásicos CCTV. Moxa integra en su solución cámaras de alta resolución en streaming con videometría, incluyendo escenarios de modificación de cámara, detección de líneas y movimiento de objetos. Además de servidores de video y almacenamiento.

VIVOTEK



Vivotek es una compañía de soluciones de vigilancia IP. Vende kits completos para distintos escenarios (vigilancia interior, exterior, tiendas etc) y se compone de cámaras, NVR (Network Video Recorder), y software para visualizar los videos.

2.5.2 Tipo Técnico

ENCRIPTACIÓN	
SOPHOS	Sophos SafeGuard cifra el contenido tan pronto se crea. Synchronized Encryption protege los datos de forma proactiva mediante la validación continua del usuario, la aplicación y la integridad de seguridad de un dispositivo antes de permitir el acceso a datos cifrados.
STEGANOS SAFE	Protege archivos y carpetas en el disco local, en memorias USB, CDs, DVDs, HDs externos y también en la nube (Dropbox, Google Drive y Microsoft OneDrive). Este cofre virtual utiliza algoritmo AES-XES de 384 bits para encriptar los archivos.
INTERCRYPTO	Ofrece 17 algoritmos distintos de encriptación, soporta PKI, borrado seguro, generador de contraseñas, encripta el texto copiado, tiene clave pública criptográfica, doble factor de autenticación, encriptación de ficheros etc.
LOGS DE AUDITORÍA	
LOGTRUST	Un log de auditoría es un documento que registra eventos. Logtrust ha diseñado un producto web para esta problemática, capaz de ingestar de distintas fuentes a gran velocidad y procesar en tiempo real y mantener estos logs en el tiempo.
SPLUNK	Splunk al igual que Logtrust provee un servicio similar. Aporta integración con terceros y un gran soporte de la herramienta.

IDS

SNORT	Snort es un NIDS (Network Intrusion Detection System). Busca detectar anomalías que inicien un riesgo potencial, tales como ataques de denegación de servicio, escaneadores de puertos o intentos de entrar en un ordenador, analizando el tráfico en la red en tiempo real. Para ello, analiza todos los paquetes, buscando en ellos patrones sospechosos
TRIPWIRE	Tripwire es un HIDS (host-based intrusion detection system), que a diferencia de NIDS, revisando las actividades en la máquina (host). Provee soluciones para industria como la protección contra interrupciones operacionales, securización automática, y correlación de configuraciones de debilidades y vulnerabilidades con estándares.

ANTIVIRUS

KASPERSKY	La solución de ciberseguridad industrial de Kaspersky está diseñada específicamente para proteger complejos entornos industriales compuestos por diversos sistemas privados. Su antivirus protege de virus y spyware
CIM - PHOENIX CONTACT	Sin tener que descargar archivos de patrones de virus, CIM reconoce si los sistemas basados en Windows como sistemas de control, unidades de mando o PC han sido manipulados, por ejemplo por software malintencionado.
SYSMANTEC	Sysmantec al igual que Kaspersky tiene una gran variedad de software para ciberseguridad. Ambos están haciendo un esfuerzo en la securización de entornos industriales a través de sus múltiples tecnologías, siendo sus antivirus uno de los más conocidos.

IMAGENES EN SERVIDOR

RACKSPACE	Rackspace Cloud provee una sencilla interfaz para restaurar y clonar imágenes a sistemas, facilitando de esta manera el despliegue y recuperación de entornos.
WINDOWS SERVER	En las versiones más actuales de Windows Server se permite recuperar el sistema a partir de un servidor externo.

TARJETAS INTELIGENTES

INFINEON	Infineon ha diseñado una serie de tecnologías y estándares abiertos (Cipurse) en el entorno de tarjetas de seguridad. Algunas de sus tecnologías se aplican a pagos, comunicaciones móviles, comunicación near-field, identificación gubernamental, usb tokens, ticketing de transportes, pay-tv, autentificación etc.
VERSASEC VSEC:CMS	SCMS o CMS es el sistema gestión de tarjetas de seguridad. Versasec provee una suite SCMS con todas las herramientas necesarias

SISTEMAS DE DEVOLUCIÓN DE LLAMADA TELEFÓNICA

CISCO CALLMANAGER	Cisco CallManager integra la característica Call Back la cual te permite recibir notificaciones de devolución de llamada a través de tu telefono IP Cisco.

BACKUPS DE DATOS

COMMVAULT	Commvault permite mantener copias de seguridad de bases de datos, ficheros, aplicaciones, endpoints y máquinas virtuales. Todo esto desde una solución integrada y centralizada.
ACRONIS	El software de Acronis crea un "full-image backup" es decir, obtiene una captura completa del sistema, no solo de los ficheros. Además encripta y comprime los backups.

2.6 ARQUITECTURAS

2.6.1 RAMI 4.0 y la seguridad

La seguridad actúa como un esqueleto que mantiene juntos todos los elementos estructurales dentro de RAMI4.0, y como resultado el diseño de la Industria 4.0. **RAMI4.0** describe los elementos claves de un objeto/activo basado en el uso de un modelo de capas en tres ejes, como se observa en la siguiente figura:

Esta estructura permite que los aspectos relevantes de un activo en particular ser presentados en cualquier punto a lo largo del ciclo de vida, así como permitir complejas interrelaciones. Los tres ejes son:

- **Eje de arquitectura (capas):** Compuesto de seis capas diferentes indicando la información desde el activo.
- **Eje de procesos (flujo de valor):** Describe las diversas etapas dentro de la vida de un activo y el proceso de creación de valor basado en IEC 62890.
- **Eje jerárquico (niveles jerárquicos):** Asigna los modelos funcionales a niveles individuales según DIN EN 62264-1 y DIN EN 61512-1.

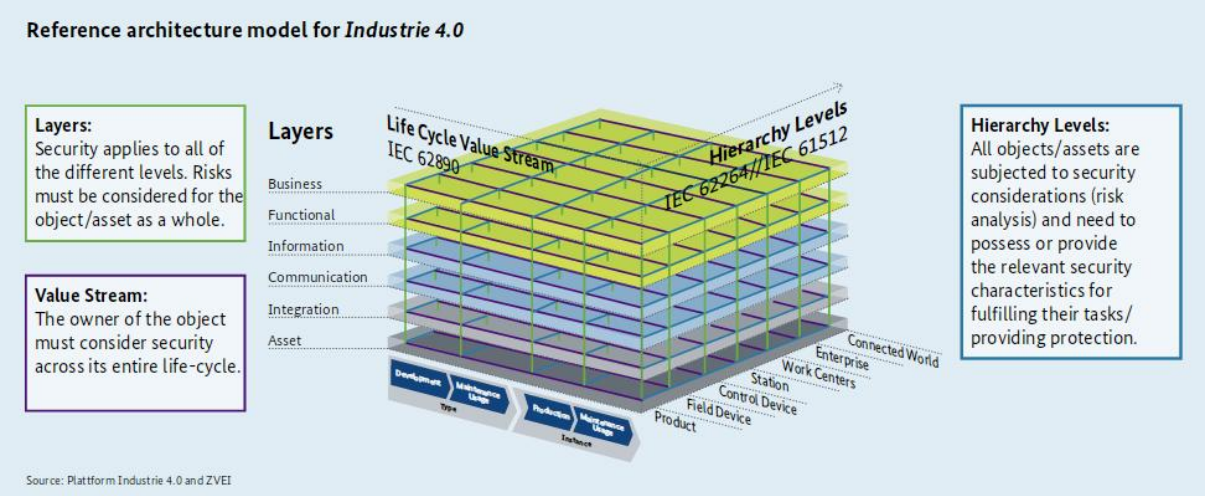


ILUSTRACIÓN 20: MODELO DE LA ARQUITECTURA DE REFERENCIA PARA LA INDUSTRIA 4.0[20]

La seguridad en RAMI4.0 está embebida y se integra con la propia naturaleza del mismo. No se representa como una capa individual o nivel de jerarquía, pero tiene impacto con todo el ciclo de vida en las capas y a todos los niveles jerárquicos.

2.6.2 Aspectos de seguridad en las administrations shells

Una de las actividades en marcha por WG3 **"Security of networked systems"** de la plataforma Industrie 4.0 es abordar la cuestión de cómo debe ser un modelo de seguridad para la *administration shell*[21] de activos y si dicho modelo de seguridad es suficiente para proteger todo el componente I4.0.

En primer lugar, debe manifestarse que los requisitos de seguridad dependen siempre del caso de uso real, es decir, deben ser el resultado de un proceso de análisis de riesgos. Las capacidades de seguridad, por otra parte, deben ser descritas como parte del modelo de activos.

En cuanto a las **capacidades de seguridad**, se han identificado los primeros temas clave necesarios para proteger la *shell* de administración de activos y sus modelos. Estos temas son:

- Identidades seguras (autenticidad).
- Comunicación segura (confidencialidad, integridad) en la negociación de conexiones de end-to-end (secciones 2.1 y 6.2), lo cual adquiere especial importancia para la comunicación entre empresas.
- Acceso de información segura (autorización, RBAC).
- Registro-logging (auditoría).

[20] Security en RAMI4.0 - Plataform Industrie 4.0

[21] Network-based Communication for Industrie 4.0 – Proposal for an Administration Shell

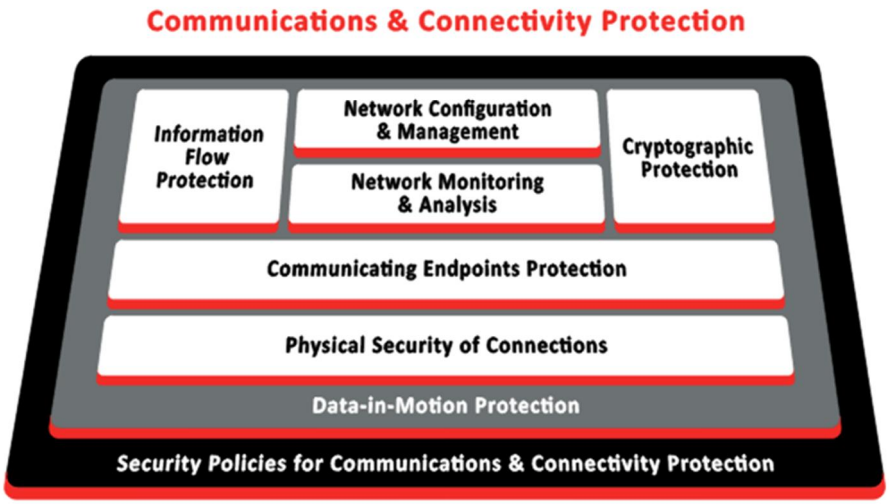


ILUSTRACIÓN 21: STACK DE COMUNICACIÓN DE LOS DATOS Y SUS CAPAS A SECURIZAR

Aún debe ser aclarado si las capacidades de seguridad deben formar parte del modelo de comunicación o del modelo de seguridad. Un ejemplo es que las **reglas de acceso a la información** deberían formar parte del modelo de comunicación para tener siempre disponible la información de autorización junto con la información a proteger.

Cómo autenticar la identidad de un socio, es decir, las medidas técnicas (por ejemplo, certificado, nombre de usuario / contraseña, cadena de confianza) y los requisitos de seguridad reales podrían ser definidos fuera del modelo de comunicación. Eventualmente, la comunicación necesita saber si una identidad específica es auténtica o no. Esto significa que la autenticidad puede y debe por lo menos ser cuantificada como una propiedad.

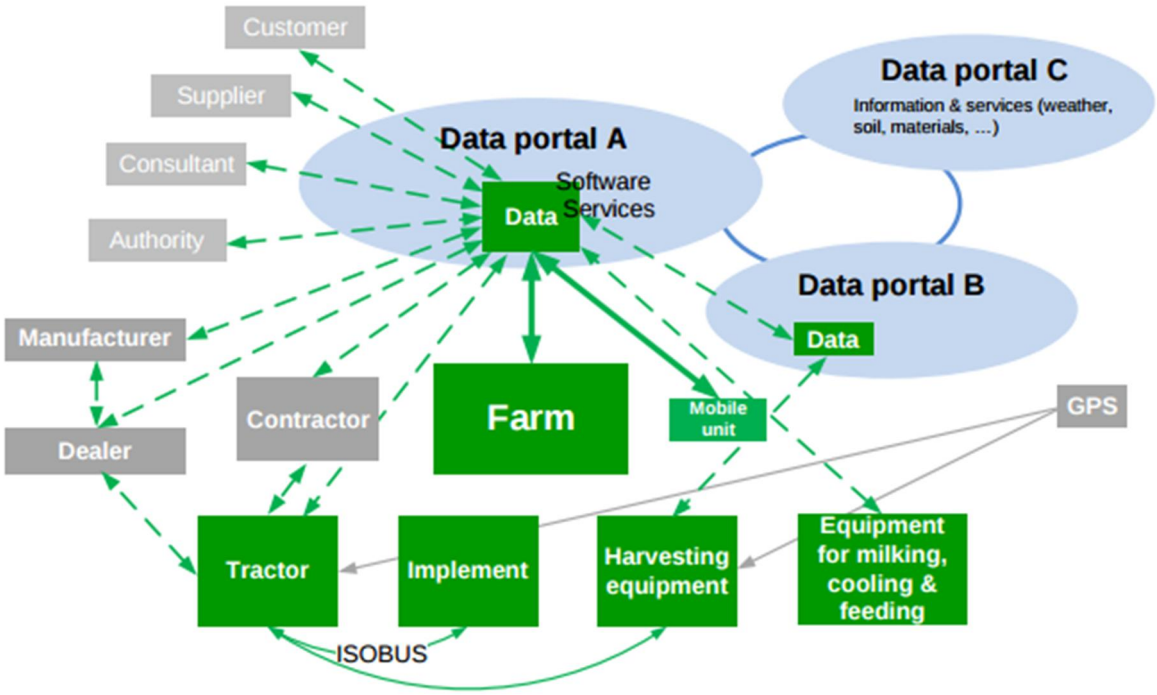
Respecto a las **medidas criptográficas**, el estado del arte evoluciona constantemente -a la vez que la rotura de cifrado-. Esto se aplica a todos los aspectos, a la autenticación de los interlocutores de comunicación, a la encriptación del contenido de la comunicación, a la autorización del acceso a los datos y a la protección de la autorización y logging de la información. Sin embargo, a diferencia de la calidad del servicio, no hay métricas acordadas para describir el nivel de calidad necesario/ofrecido de los mecanismos criptográficos para asegurar una comunicación segura. Por ejemplo, IEC 62443 recomienda la definición de niveles de seguridad. La implementación actual de dichos niveles de seguridad es específica de ciertos casos de uso, empresas o dominios. Para garantizar la interoperabilidad en toda la industria 4.0 se necesitan niveles de seguridad o políticas de seguridad normalizados, lo que hace que la seguridad alcanzable sea comprensible tanto para los fabricantes como para los clientes, pero también para las negociaciones máquina a máquina.

Esto significa que, al igual que la calidad del servicio, se requiere un conjunto acordado de propiedades cuantificables, para que los componentes de Industrie 4.0 negocien los niveles de seguridad para el intercambio de datos como parte de su contratación. Este es el camino para definir la confiabilidad de un componente. Una decisión clave será la medida en que los niveles de seguridad serán abstraídos de la tecnología subyacente (criptográfica), es decir, si los algoritmos o longitudes de clave se referenciarán directamente o no.

3. SECTORES Y APLICACIONES

3.1 AGROALIMENTACIÓN Y BIO

En el contexto de la agricultura y la Industria 4.0 se define el concepto **Digital Farming**.[22] Digital Farming describe la evolución de la agricultura y la ingeniería agrícola, desde la agricultura de precisión, hasta los sistemas de producción agrícola conectados y basados en conocimiento. Además de hacer uso de las **tecnologías de Precision Farming**, recurre a redes inteligentes y herramientas de gestión de datos. El objetivo es utilizar toda la información y los conocimientos disponibles para permitir la automatización de procesos sostenibles en la agricultura.



Esto implica un uso intenso de de los datos, por lo que se deberá asegurar los tres principios fundamentales de seguridad (**integridad, confidencialidad y disponibilidad**).

Además es un trabajo asociado a maquinaria pesada, por lo que los conceptos de *Safety* cobran una importante relevancia, no solo para los operarios, sino que también para los posibles impactos en el medio ambiente.

El gobierno australiano es bien conocedor de estos problemas ya que son un gran productor y exportador agrícola. Los agricultores y ganaderos poseen más de 135.000 granjas que cubren el 61% de su superficie[23]. Por ello, anualmente la Agencia **"Safe Work Australia"** publica el informe "Work Health And

[22] http://cema-agri.org/sites/default/files/CEMA_Digital%20Farming%20-%20Agriculture%204.0_%2013%2002%202017.pdf

[23] New reference reveals facts about Australian farming Retrieved 30 January 2011

Safety In The Agricultural Industry"[24] lo que nos permite tener una visión extrapolable a los problemas y mejoras de *Safety* a nivel mundial.

3.2 AUTOMOCIÓN

Los estándares y las buenas prácticas de la industria contribuyen a **entornos de automoción más seguros**. La seguridad en automoción es una ciencia probabilística con riesgos y componentes medidos e identificados para mitigar esos riesgos. Sin embargo la seguridad computacional no es probabilístico. Las amenazas provienen de una variedad de fuentes, incluyendo intencionalmente maliciosas y no intencionalmente malignas.

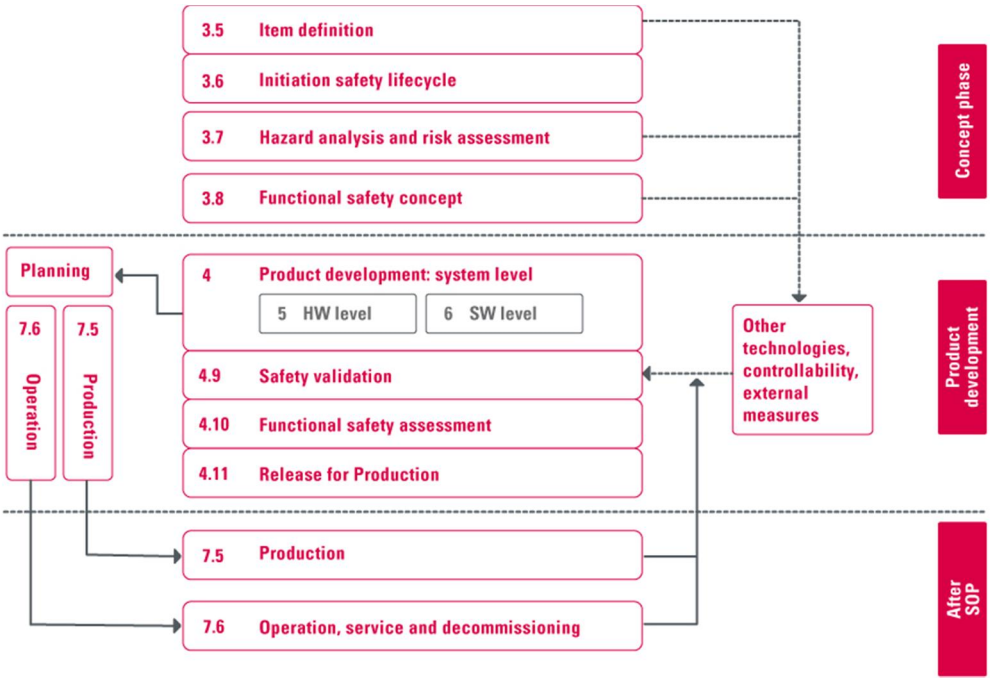
El objetivo de la seguridad es, por lo tanto, mitigar las amenazas antes y después de que ocurran. El escenario de la seguridad tiene que mitigar estas amenazas durante todo el ciclo de vida del producto, desde las decisiones de diseño tempranas hasta la fabricación y cierre.

Para ello existen frameworks como **SDL25 (Security Development Lifecycle)**, que permite al desarrollador del producto tratar la identificación de amenazas, utilizar mecanismos para mitigar las amenazas, implementar procesos para fabricar el producto, entender cómo manejar las hazañas y replicar aprendizajes para futuros productos.

[24]http://www.safeworkaustralia.gov.au/sites/SWA/about/Publications/Documents/976/whs-in-the-agricultural-industry.pdf

[25] https://www.mcafee.com/tw/resources/white-papers/wp-automotive-security.pdf

Desde el punto de vista de producto, los fabricantes y proveedores deben ser capaces de demostrar a los clientes y licenciadores que los sistemas electrónicos entregarán la funcionalidad requerida de manera segura y fiable, a pesar de la creciente complejidad. En la siguiente figura se expone la **ISO 26262, "Safety Lifecycle"**.



3.3 MADERA / FORESTAL

La industria forestal es una industria con grandes riesgos y ha sufrido un gran número de muertes y lesiones relacionadas con el trabajo a lo largo de los años.

Es por ello que existeN una serie de **códigos de buenas prácticas**[26] que se aplica a cualquier persona que tenga un deber en las circunstancias descritas en el código - que puede incluir a los empleadores, los empleados, los autónomos, los directores de contratos, los propietarios de edificios o plantas, etc.

Por lo general, estos códigos de seguridad llevan años implantados en esta industria. La Industria 4.0 permitirá una mayor comunicación en cada uno de los procesos, por lo que esta mejora se tendrá que adherir a los requerimientos mínimos de *Security* de los datos.

[26] Approved Code of Practice for Safety and Health in Forest Operations - 2012

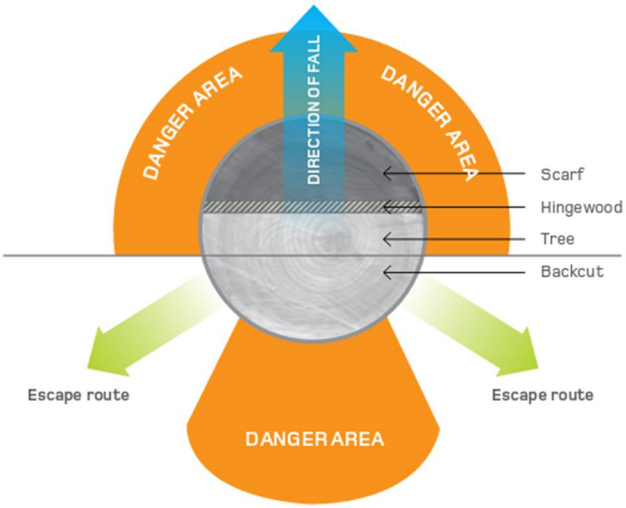


ILUSTRACIÓN 22: RUTAS DE ESCAPE DE LA CAÍDA DE UN ÁRBOL

3.4 NAVAL

La **protección de los puertos y su infraestructura especializada** es una preocupación creciente debido al aumento de su tamaño, así como los riesgos humanos y ambientales que plantean. Un ataque terrorista marítimo a gran escala es actualmente más probable porque los sistemas de Control Supervisor y Adquisición de Datos (SCADA) no son lo suficientemente seguros y los puertos no disponen de tiempo y dinero suficientes para gastar en invertir en algo más que la seguridad mínima.

Al igual que el sector del automóvil, el sector Naval debe asegurar **todo el ciclo de vida**, desde la fabricación, donde se maneja las mismas problemáticas, hasta el despliegue y uso. Para ello es necesario tener políticas y directivas de seguridad en puertos y alta mar.

En el informe *UK Marine Security Market Report-2013* identifican la siguiente tabla a partir de una serie de subsectores en el dominio de *Safety y Security*:

SUB-SECTOR	DRIVERS	POSIBLES OPORTUNIDADES	TECNOLOGÍA EMERGENTE / OPORTUNIDAD DE INNOVACIÓN
Vigilancia Marítima y Vigilancia Naval	Anti-Terrorismo Contenido ilegal Inmigración	Sistemas automáticos	UAVs CCTV tecnología de teledetección Radar HF Radar pasivo navegación electrónica

Observación y Ciencias Marítimas	Investigación ambiental cambio climático	Sistemas automáticos	Vehículos submarinos
Comunicaciones	Mayor ancho de banda vía satélite Conectividad VHF mejorada	Aplicaciones que favorecen el correo electrónico y los comunicados de texto.	Protección cibernética Mejora de las tecnologías SATCOM para el equipamiento GMDSS a bordo, (INMARSAT-C) Satélite AIS
Seguridad portuaria	Anti-Terrorismo	Programas de seguridad anti-buceo	Sistema submarino autónomo
Sistemas de gestión marítima	Convergencia de sistemas Ciencias económicas	Desarrollo de software de gestión	Aplicaciones basadas en el intercambio ágil de información
Datos y Seguridad Cibernética	Transparencia Lucha contra el crimen organizado	Desarrollo de software de seguridad	Desarrollo de nuevos conceptos sobre SCADA
Seguridad en alta mar	Monitoreo ambiental Vigilancia de la pesca Control de polución Antiterrorismo		Radar AIS Sonar
Seguridad en mar territorial	Vigilancia Monitoreo de Embarcaciones Inmigración ilegal		Mejora del rendimiento de radar y AIS. Sistemas de monitoreo de buques contra la intrusión y falla del sistema
Seguridad en Aguas Internacionales	Políticas nacionales Políticas internacionales	Colaboraciones internacionales	Protección de buques y sistemas de endurecimiento Armas no letales

3.5 METALMECÁNICO

El sector metalmecánico engloba a un heterogéneo conjunto de empresas que trabajan en torno a la producción y el procesado del metal y que a su vez trabajan en actividades de automoción, naval, marítimo, energías renovables, construcciones y estructuras metálicas, carpintería de metal…

Por el tipo de operaciones que se realizan y por los equipos y maquinaria con los que se trabaja en las empresas del sector metalmecánico, en los conceptos de safety & security tienen una gran relevancia todos los **aspectos relacionados con la seguridad de las personas**, ya que la actividad productiva expone a los trabajadores a actividades que, si no se ejecutan de un modo adecuado, pueden suponer un riesgo importante para su salud. Las empresas del sector son muy conscientes de la importancia de la prevención de riesgos laborales y las soluciones para reducir el riesgo de sus trabajadores tienen gran importancia para ellos.

Los **accidentes típicos** en estos sectores son aquellos producidos fundamentalmente por golpes con objetos y herramientas, sobreesfuerzos y proyecciones de fragmentos o partículas. Otra fuente importante de riesgos para la salud en el trabajo en este sector son el ruido generado por el funcionamiento de la maquinaria o de las herramientas manuales y los gases y partículas generadas en las operaciones de producción. En aquellas industrias en las que existan procesos de soldadura, las radiaciones no ionizantes pueden producir quemaduras o lesiones a nivel ocular.

Las nuevas tecnologías están impulsando mejoras efectivas en la gestión de la seguridad laboral. Los **wearables y redes de sensores automatizados** son algunas de las soluciones más comunes y que facilitan el seguimiento y monitorización de los operarios, de sus actividades y del entorno en el que trabajan. Así por ejemplo, se despliegan redes de sensores que detectan y alertan de situaciones peligrosas, como los nuevos sistemas de robótica colaborativa que pueden trabajar detectar la presencia de trabajadores o de otros equipos en su entorno y actuar en consecuencia. Es común el uso de sensores para detección de gases o sustancias peligrosas o dañinas en el ambiente de trabajo; con la evolución de las **tecnologías de sensado y de comunicaciones** inalámbricas, la tendencia es que estos sensores se instalen lo más cerca posible del operario, integrados en el propio puesto de trabajo o en los equipos de protección individual.

A continuación se muestran algunos ejemplos de soluciones que se están implantando en el sector metalmecánico para mejorar la seguridad de sus operaciones:

- **Solución wearable de Intel y Honeywell**[27]: Intel y Honeywell han creado una prueba de concepto genérica para cualquier tipo de trabajador que une diversas tecnologías como la detección de actividad, detección de gestos o monitorización de variables ambientales, entre otras. Estos dispositivos se conectan con un servicio en la nube en el que se analizan los datos obtenidos. Es una solución que está en el estado de prueba de concepto y que sirve para monitorización del estado de operarios, detección de parámetros ambientales peligrosos (p. ej. gases tóxicos), además de para la obtención en tiempo real de tiempos de actividad para optimización de operaciones.

[27] http://www.intel.es/content/www/es/es/industrial-automation/industrial-applications/honeywell-industrial-wearables-solution-brief.html

- **WearKinetic**[28]: Wearable orientado a monitorizar si los operarios realizan correctamente actividades de carácter físico en cuanto a las posturas que adoptan, peso que levantan, etc. Dispone de interfaces de visualización para detectar aquellos trabajadores con un mayor riesgo de lesión. Por ejemplo, han implementado un caso de uso en Crane Worldwide Logistics. Esta solución persigue la reducción de riesgos laborales a través de la monitorización de los operarios con trabajos físicos intensos.
- **Daqri Smart Helmet**[29]: Casco diseñado para presentar a los trabajadores información a través de una interfaz de realidad aumentada en su visor. Puede presentar información de diversos sensores en tiempo real (monitorización de concentración de gases, estado de la maquinaria, etc.), actuar como sensor empleando las cámaras térmicas y de infrarrojos incorporadas, o para el apoyo remoto de expertos en tiempo real y comunicación con los trabajadores. Esta solución presenta información de sensores y estado de los procesos, monitorización de actividad a través de sensores en el casco.

3.6 TEXTIL/MODA

La industria textil consiste en una serie de elementos dedicadas a la hilatura, el tejido, el teñido, la impresión, el acabado y otros procesos que se requieren para convertir la fibra en una tela acabada o prenda. Hay varios problemas de seguridad y salud asociados con la industria textil.

Los principales problemas de *Safety* y salud en la industria textil se pueden diferenciar en:

- **Exposición a productos químicos:** Los trabajadores de la industria textil están expuestos a una serie de productos químicos, especialmente aquellos dedicados a las actividades de teñido, impresión y acabado.
  En las operaciones textiles se utilizan sustancias químicas a base de bencidina, abrillantadores ópticos, disolventes y fijadores, agentes que liberan formaldehído y retardantes de llama que incluyen compuestos organofosforados.
- **Exposición al ruido:** Se han observado altos niveles de ruido en la mayoría de las fábricas dedicadas a la industria textil, en particular en los países en desarrollo. A largo plazo, se sabe que la exposición a altos niveles de ruido daña el tímpano y causa pérdida auditiva.
  Otros problemas como fatiga, absentismo, molestia, ansiedad, reducción de la eficiencia, cambios en el pulso y la presión arterial, así como trastornos del sueño también se han detectado a causa de la exposición continua al ruido. La falta de mantenimiento de la maquinaria es una de las principales razones detrás de la contaminación acústica. Aunque causa efectos graves para la salud, la exposición al ruido es a menudo ignorada porque sus efectos no son inmediatamente visibles.
- **Problemas ergonómicos:** Los problemas ergonómicos se detectan en la mayoría de las fábricas dedicadas a actividades textiles en la India. La mayoría de estas unidades tienen un ambiente de trabajo inseguro y poco saludable para los trabajadores.
  Los trabajadores se enfrentan una serie de problemas como muebles inadecuados, ventilación e iluminación inadecuadas y falta de medidas de seguridad eficientes en caso de emergencias.

[28] http://wearkinetic.com/

[29] https://daqri.com/products/smart-helmet.html

Además corren el riesgo de desarrollar diversas enfermedades profesionales como trastornos musculoesqueléticos como el síndrome del túnel carpiano, la tendinitis del antebrazo, la tendinitis bicapital, el dolor lumbar, la epicondilitis, el dolor de cuello, el dolor en el hombro y la osteoartritis de las rodillas. Estas cuestiones son más comunes en los países en desarrollo que en los países desarrollados.

3.7 AERONÁUTICO

La **regulación** desempeña un papel fundamental en la seguridad del sistema de aviación y es un aspecto necesario de las operaciones comerciales en una economía de mercado en funcionamiento.

Esta industria reconoce que la regulación beneficia tanto a los consumidores como a la industria proporcionando claridad y certeza para todos.

En este contexto, la IATA (*International Air Transport Association)* tiene un peso importante en la regularización de medidas de seguridad para asegurar la seguridad de los vuelos y aviones.

En este contexto se puede diferenciar:

- ***Safety* de la aviación**, se refiere a los esfuerzos que se toman para asegurar que los aviones estén libres de factores que pueden conducir a lesiones o pérdidas. Los principales fabricantes como Boeing se adhieren a todas las regulaciones de seguridad establecidas por las agencias reguladoras.
- ***Security***, es el componente que puede afectar la seguridad de los pasajeros. No se relaciona tanto con el avión en sí, sino con la obtención de inteligencia, los procedimientos de preembarque y el personal de seguridad del aeropuerto.

RASG	Estimated Departures (in millions)	Number of accidents	Accident rate (per million departures)	Fatal accidents	Fatalities
AFI	0.7	9	12.9	1	33
APAC	8.6	19	2.2	1	49
EUR	7.9	21	2.7	2	71
MID	1.1	2	1.8	0	0
PA	13.8	39	2.8	5	20
WORLD	**32.1**	**90**	**2.8**	**9**	**173**

ILUSTRACIÓN 23: TOTAL DE ACCIDENTES AÉREOS 2014[30]

En este proceso, el concepto *Safety & Security* de la Industria 4.0 tiene su foco en la manufactura. En el sector aeronáutico la asociación GAMA (General Aviation Manufacturers Association) juega un papel fundamental en esta transición. Se definen con el siguiente texto:

[30] Safety Report - ICAO 2014

"GAMA Se dedica a un propósito primordial: fomentar y promover el bienestar general, la seguridad, los intereses y las actividades de la aviación general en todo el mundo. Esto incluye promover un mejor entendimiento de la manufactura, mantenimiento, reparación y revisión general de la aviación".

3.8 TIC

El caso del sector TIC, en contraposición con el resto, tiene una **naturaleza transversal** que permite desplegar estrategias de *Security* como se ha ido explicando a lo largo de este informe, ya que la evolución de la industria hacia un paradigma 4.0 está directamente relacionado con el sector TIC.

Sin embargo, como sector individual también existen riesgos. En el dominio de *Security* de los datos existen amenazas como el hacking, phishing, pharming, spyware, virus, spam etc que son necesarios resolver con software y conocimiento apropiado. Por otra parte también existen peligros de *Safety* que aplican, aunque en menor medida que otros sectores, como el riesgo de incendios, electrocución, caídas de equipamiento pesado.

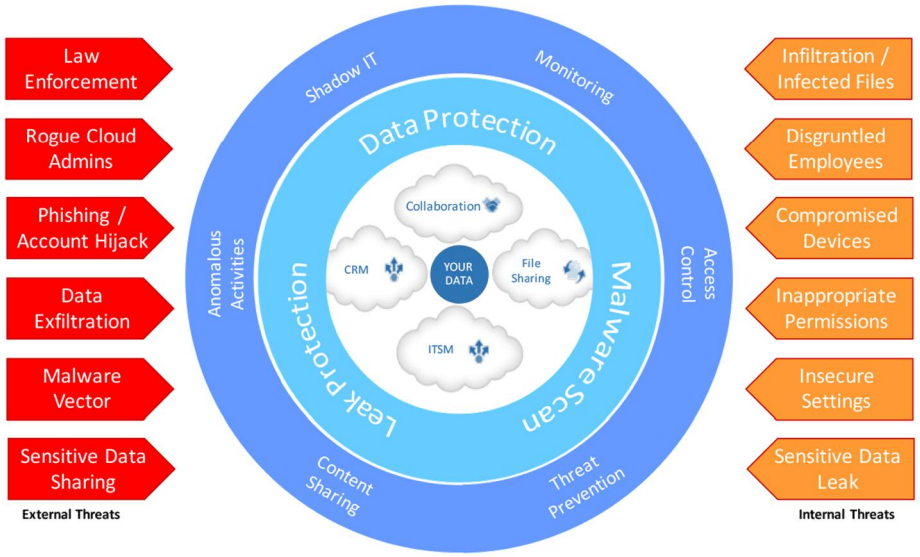


ILUSTRACIÓN 24:ESTRATEGIA DE SECURIZACIÓN PARA SISTEMAS CLOUD

3.9 ENERGÍAS RENOVABLES

Los **sistemas de energía** renovable pueden mejorar algunos aspectos de la seguridad, pero no conseguirán automáticamente a la eliminación de todo tipo de problemas de seguridad y sin duda surgirán nuevos problemas. Las fuentes de energía renovables no acarrean el problema de la disponibilidad de recursos a largo plazo que los recursos fósiles finitos y su ubicación geográfica es menos concentrada. Muchas cuestiones de seguridad relacionadas con la energía también dependen del proveedor de energía más que del recurso energético y de la existencia de instituciones y reglamentos que funcionen eficazmente.

Por tanto, la energía renovable puede afectar la seguridad energética de varias maneras. En la siguiente figura se expone un framework[31] para atacar a este problema.

3.10 PIEDRA NATURAL

Las actividades desarrolladas en este sector son susceptibles de causar enfermedades del trabajo, concepto que aglutina las enfermedades profesionales y, por otro, enfermedades relacionadas con el trabajo. Las **enfermedades del trabajo más frecuentes** son: la silicosis, la hipoacusia, los trastornos musculoesqueléticos, el enfisema pulmonar y otras patologías en menor proporción.

A las enfermedades anteriores se le añade también el nuevo reto de prevenir, detectar y reconocer los **nuevos riesgos emergentes**: nanopartículas, combinación de factores psicosociales con trastornos musculoesqueléticos o alteradores endocrinos, entre otros.

Todos estos problemas de *Safety* tratan de resolverse en diversos informes técnicos, protocolos y manuales de manipulación, posturas etc, como se puede observar en el informe "Enfermedades Profesionales y Riesgos Emergentes en el sector de la piedra natural y su prevención." o incluso certificaciones y cursos internacionales como el **MIA+BSI's Natural Stone Safety Program**.

Además, el proceso el propio proceso productivo tiene otros riesgos de *Safety* compartido con sectores como el forestal.

[31] Security aspects of future renewable energy systems–A short overview

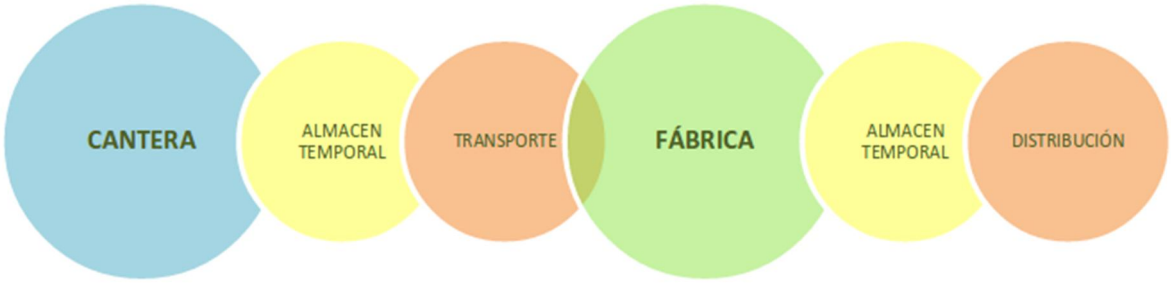


ILUSTRACIÓN 25: PROCESO PRODUCTIVO EN EL SECTOR DE LA PIEDRA NATURAL

4. CONCLUSIONES

En el contexto de la Industria 4.0 hay una variedad de desafíos a solventar. Aparte de los retos técnicos, las soluciones de seguridad exitosas también tendrán que abordar **cuestiones comerciales, psicológicas y educativas**.

Por ejemplo, actualmente la industria carece de plataformas operativas totalmente estandarizadas para implementar soluciones de seguridad adecuadas que se han adaptado a los requisitos específicos de la industria en términos de su implementación y costo, de modo que no se consideren simplemente controladores de costes.

A menudo hay poco que se puede hacer para ampliar o actualizar la infraestructura existente, especialmente porque muchas soluciones de seguridad fueron desarrolladas originalmente para otras industrias o aplicaciones. Por otra parte, la **conciencia de seguridad** a menudo juega un papel clave, especialmente en lo que respecta a las cuestiones de seguridad de TI. Actualmente hay demasiadas discrepancias con respecto al nivel de conciencia de seguridad en diferentes industrias.

Teniendo en cuenta que Industria 4.0 implicará un **aumento de la creación de redes y la cooperación entre varios socios diferentes** en la cadena de valor, será necesario que tengan un mayor grado de confianza mutua (seguridad y confianza).

Los fabricantes de maquinaria y plantas están cada vez más conscientes del potencial valor añadido del software, lo que da como resultado un fuerte aumento en el número de componentes de software que se encuentran en las instalaciones de fabricación y maquinaria.

Sin embargo, todavía se sabe poco sobre las amenazas de TI. La seguridad de TI industrial sólo ha comenzado a ser discutida en la industria de la automatización desde el **debate público que rodea el malware**, como Stuxnet, Duqu o Flame.

Por otra parte, el software también está desempeñando un papel cada vez más importante en la entrega y el mantenimiento de la seguridad, pero esto es algo que todavía no ha sido debidamente asumido por los procesos de fabricación y donde las soluciones disponibles todavía tienen que ser implementados.

En términos generales, Industria 4.0 requerirá un **enfoque mucho más proactivo de la seguridad** que lo que ha sido hasta ahora (especialmente en lo que se refiere a la seguridad por diseño). Actualmente las cuestiones de seguridad a menudo sólo se plantean de forma reactiva una vez que el proceso de desarrollo ha terminado y se han producido problemas específicos de seguridad.

Sin embargo, esta **tardía aplicación de las soluciones de seguridad** es costosa y a menudo no logra ofrecer una solución permanente al problema real. En consecuencia, la seguridad no puede simplemente ser desglosada en componentes funcionales, sino que debe ser abordada como un proceso.

A fin de lograr tiempos de respuesta rápidos, también es importante prestar apoyo mediante el seguimiento y los intercambios de información intersectoriales completos.

Por el momento, no existe un control suficiente de los indicadores de evaluación de riesgos, en particular en lo que respecta a la seguridad industrial de TI, y se intercambia poca o ninguna información sobre incidentes de seguridad y protección. La proactividad en estas áreas ayudaría a detener la propagación de virus o ciberataques indiscriminados.

5. BIBLIOGRAFÍA

ARTÍCULOS E INFORMES DE REFERENCIA

- Deloitte: Industry 4.0 Challenges and Solutions for the digital transformation and use of exponential technologies
- Deloitte: Global Cyber Executive Briefing: Manufacturing
- US sees jump in cyber attacks on critical manufacturing infrastructures, report by Jim Finkle
- Smarter Security For Manufacturing in the Industry 4.0 ERA – Sysmantec
- Recommendations for implementing the strategic initiative INDUSTRIE 4.0 - Final report of the Industrie 4.0 Working Group
- Infraestructuras críticas y sistemas industriales - Juan Francisco Bolívar
- FireEye 2016 ICS Vulnerabilities Trend Report: Missed Warnings, Exposed Industrial Environments
- Industrial Control Systems – Shodan
- Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
- Recommendations for implementing the strategic initiative INDUSTRIE 4.0, 2013, Acatech – National Academy of Science and Engineering
- La Ciberseguiridad en la Industria 4.0 – Incibe
- Smarter Security For Manufacturing in the Industry 4.0 ERA – Sysmantec
- Industrial Demilitarized Zone Design Principles - Rockwell Automation
- FireEye 2016 ICS Vulnerabilities Trend Report: Missed Warnings, Exposed Industrial Environments
- Security en RAMI4.0 - Plataform Industrie 4.0
- Network-based Communication for Industrie 4.0 – Proposal for an Administration Shell
- Approved Code of Practice for Safety and Health in Forest Operations - 2012
- Safety Report - ICAO 2014
- Security aspects of future renewable energy systems–A short overview

PÁGINAS WEB CONSULTADAS

- "Implementation Strategy Industrie 4.0 - Report on the results of the Industrie 4.0 Platform". 2016. Bitkom, VDMA, ZVEI. http://www.zvei.org/Publikationen/Implementation-Strategy-Industrie-40-ENG.pdfhttp://www.zvei.org/Publikationen/Implementation-Strategy-Industrie-40-ENG.pdf
- Recomendación ITU-T Y.2060, ITU, 2012, https://www.itu.int/rec/T-REC-Y.2060-201206-I/es

- New reference reveals facts about Australian farming Retrieved 30 January 2011
- http://www.safeworkaustralia.gov.au/sites/SWA/about/Publications/Documents/976/whs-in-the-agricultural-industry.pdf
- https://www.mcafee.com/tw/resources/white-papers/wp-automotive-security.pdf
- http://www.intel.es/content/www/es/es/industrial-automation/industrial-applications/honeywell-industrial-wearables-solution-brief.html
- http://wearkinetic.com/
- https://daqri.com/products/smart-helmet.html