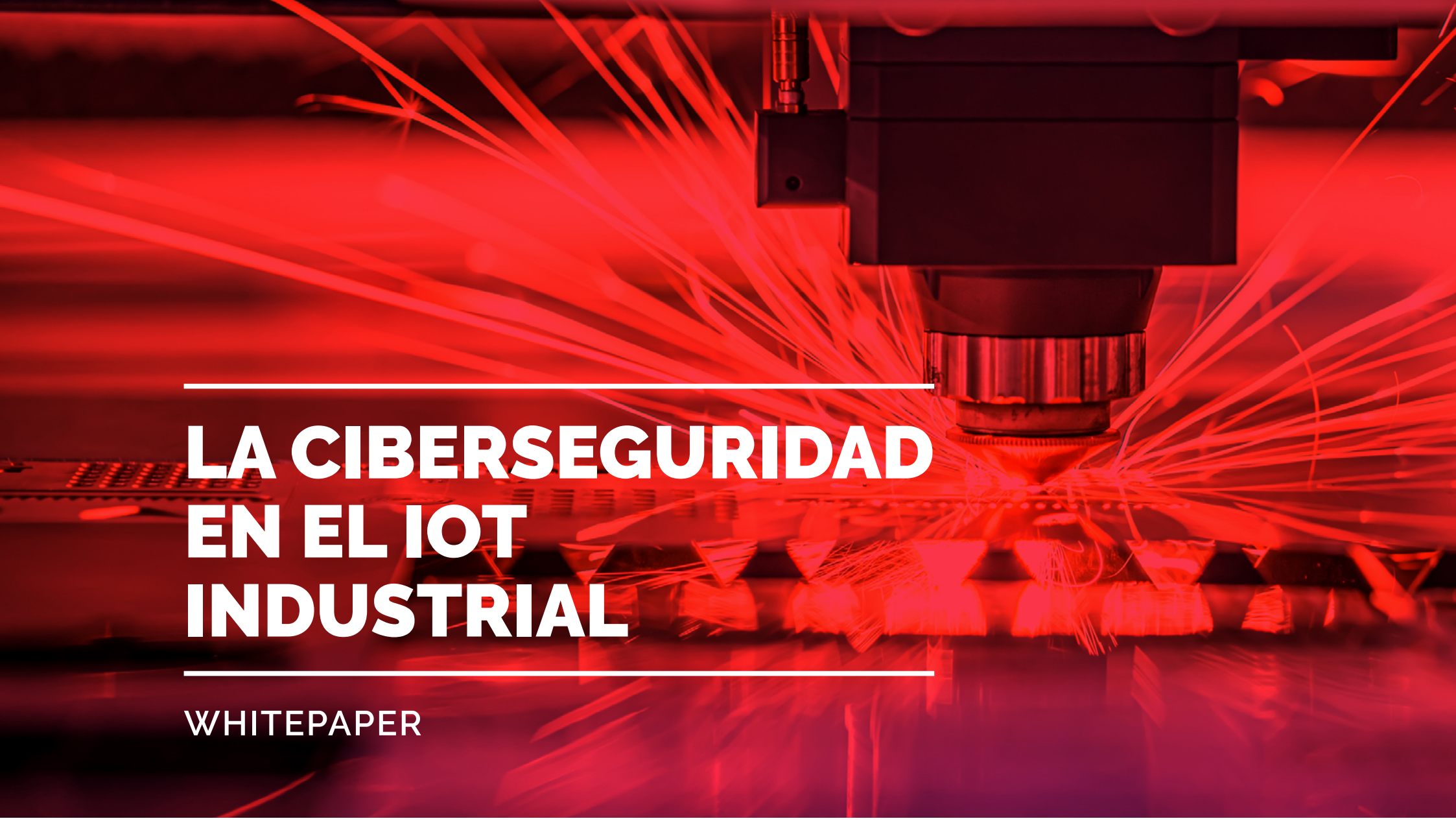


LA CIBERSEGURIDAD EN EL IOT INDUSTRIAL

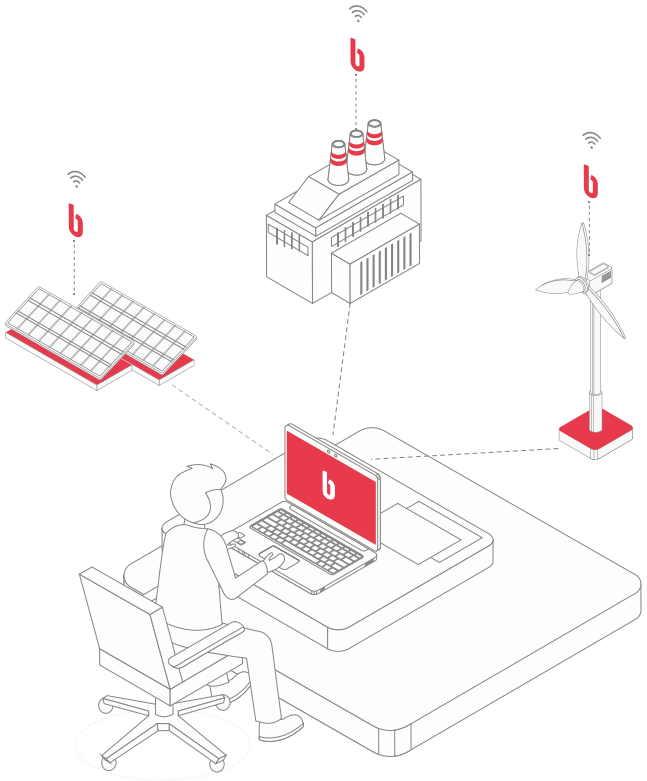
WHITEPAPER

EDITADO POR:

David Purón, CEO de Barbara IoT

Juan Pérez-Bedmar, VP Marketing y Ventas de Barbara IoT

barbara



ÍNDICE

RESUMEN EJECUTIVO

El rápido crecimiento del Internet de las Cosas (hoy hay ya más de 12 mil millones de dispositivos conectados) ha traído consigo un importante aumento de ciberataques.

Los riesgos de ciberseguridad son precisamente un freno y a la vez un reto a superar en los despliegues de IoT en entornos industriales. Las carencias en materia de ciberseguridad de estos entornos los han convertido en un claro objetivo para los cibercriminales.

El impacto económico que esto tiene sobre las empresas es enorme: robo masivo de datos, ataques de denegación de servicio (DoS), bloqueo o "rapto" de dispositivos...

El panorama de amenazas ha evolucionado hasta tal punto que se da por sentado que los ciberataques contra la mayoría de las empresas serán inevitables. No es una cuestión de si ocurrirá sino de cuándo lo hará.

En esta situación, los dispositivos se revelan como el eslabón más débil de la cadena de seguridad de IoT. Contra ellos se focaliza gran parte de los ataques ya que, por lo general:

- Tienen **capacidades de computación limitadas** dejando poco espacio para mecanismos de seguridad robustos
- Su **heterogeneidad** dificulta la existencia de métodos y protocolos de protección estándar
- Usan **contraseñas débile**s, adivinables o accesibles.
- Tienen **interfaces inseguras**
- Usan **servicios de red inseguros**

Los dispositivos son el eslabón más débil del IoT. Es crucial seguir normativas, recomendaciones y guías de diseño de los diferente organismos expertos

Protegerse frente a las ciberamenazas requiere desarrollar y poner en práctica medidas en diferentes áreas:

- **En el aspecto técnico**, la metodología STRIDE ayuda a asentar un buen marco de análisis sobre las amenazas a controlar
- **En el aspecto procesal,** el NIST americano propone cinco funciones orientadas a la reducción de riesgos de ciberseguridad en infraestructura crítica
- **En el aspecto presupuestario** es muy aconsejable establecer una mecanismo de medición del ROI mediante KPIs claros

Cabe destacar las iniciativas tanto legislativas (como las de EEUU, la UE y Australia) como de organismos internacionales de estandarización (como las del IEC, el Industrial Internet Consortium, OWASP, la GSM y la IoT Security Foundation).

Estas iniciativas dan una guía de cómo diseñar y desarrollar políticas de ciberseguridad para soluciones IoT.

En el presente whitepaper exploramos y profundizamos en todos estos aspectos, dando una visión completa del estado actual de la ciberseguridad en el IoT industrial.

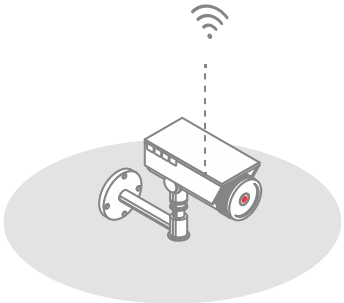
EL ESTADO DE LA CIBERSEGURIDAD EN EL IOT INDUSTRIAL

EL INTERNET DE LAS COSAS Y LA SEGURIDAD

La adopción en los últimos años del "Internet de las Cosas", pese a ser un término relativamente joven (año 1999), ha sido tal que hoy contamos con más de 12 billones (12 mil millones) de cosas conectadas en el mundo y se espera que para el 2025 se alcance los 30.000 millones de dispositivos conectados, una media de 4 dispositivos IoT, por persona.

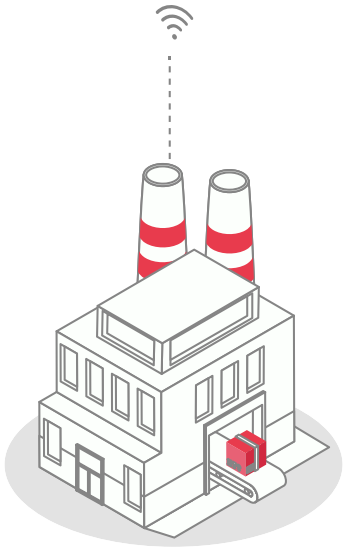
En los próximos 10 años veremos una transformación completa del mundo empresarial con fábricas inteligentes, negocios inteligentes, industrias inteligentes. Y no es porque se pueda, sino porque se debe cambiar. Nos enfrentamos a un mercado cada vez más competitivo en el que todo gira en torno a responder a la demanda al menor coste posible.

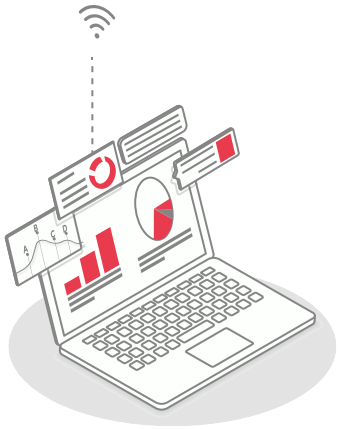
En este nuevo entorno de cosas conectadas, la multiplicación de los ciberataques ha sido exponencial. Sólo en el primer semestre del 201,9 el número de ataques a dispositivos IoT creció en un 300%.



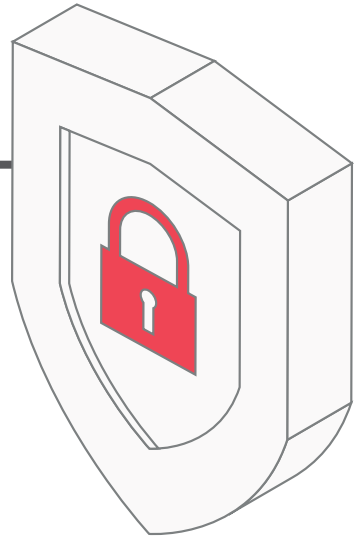
En el primer semestre del 2019, el número de ciberataques a dispositivos IoT creció en un 300%. Esto representó 2.900 millones de eventos y fue la primera vez que las cifras superaron los mil millones

(fuente: Panorama de ataques F-Secure H1 2019)





LA SEGURIDAD, EL TELÓN DE AQUILES DEL INTERNET DE LAS COSAS



En los últimos años, el panorama de los ataques ha evolucionado hasta tal punto que se da por sentado, que los ciberataques contra la mayoría de las empresas serán inevitables. Ya no se habla de prevenir los ataques sino de asumir que van a suceder. Es una cuestión de "cuándo" y no de si ocurrirá

La fragmentación y la seguridad son los dos grandes retos para la adopción masiva del Internet de las Cosas y ambos desafíos están intrínsecamente relacionados.

A pesar del nombre del Internet de las cosas (IoT), que implica una síntesis de dispositivos conectados, las tecnologías IoT **varían considerablemente dependiendo de su caso de uso**. Las empresas que desean abordar un proyecto del IoT **dependen de una gran variedad de tipos de conectividad, estándares y hardware**. Un dispositivo de IoT simple puede presentar muchas vulnerabilidades de seguridad, que incluyen autenticación débil, integración insegura en la nube así como un firmware y software desactualizado.

Las carencias en materia de ciberseguridad de estos nuevos entornos industriales y de los propios dispositivos que los conforman, hacen que estos últimos se hayan convertido en un claro objetivo para los ciber-criminales que llevan a cabo ataques como pueden ser :

- El **robo masivo de datos sensibles**
- Ataques de **denegación de servicio distribuidos** (DDoS, de sus siglas en inglés) contra servicios de terceros en Internet
- **Ataques de bloqueo o secuestro de dispositivos,** que pueden llegar a **bloquear infraestructuras críticas**
- Ataques de **manipulación de dispositivos** que pueden tener un impacto ciberfísico y causar daños materiales a la infraestructura y a usuarios.

EL DISPOSITIVO, EL ESLABÓN MÁS DÉBIL EN LA CADENA DEL IOT INDUSTRIAL

Muchos dispositivos de IoT son vulnerables porque carecen de la seguridad incorporada necesaria para contrarrestar las amenazas.

- Son dispositivos con **capacidades de computación limitadas** y restricciones de hardware, con funciones específicas que garantizan solo capacidades informáticas limitadas y dejan poco espacio para mecanismos de seguridad robustos y protección de datos
- Los dispositivos suelen utilizar una **variedad de tecnología de transmisión**. Esto puede dificultar el establecimiento de métodos y protocolos de protección estándar
- **Contraseñas débiles**, adivinables o no modificables: las nuevas variantes de malware suelen utilizar esta vulnerabilidad
- **Interfaces inseguras** del ecosistema
- **Servicios de red inseguros**: puertos abiertos que exponen el dispositivo a cualquier persona en Internet y revelan información confidencial del usuario

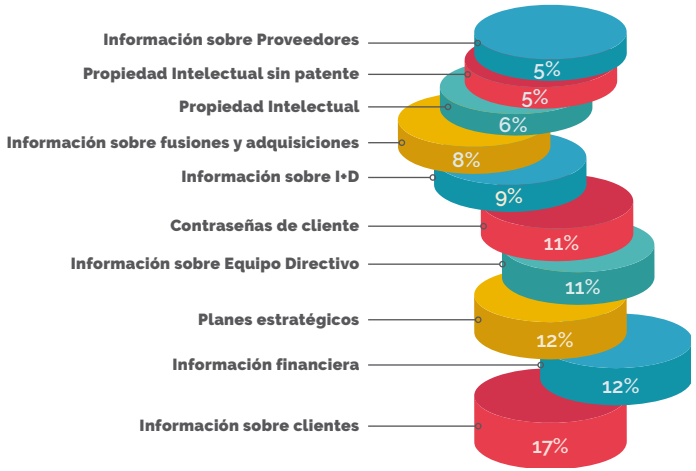
Más del 25% de los ataques identificados en las empresas en el 2020, tendrán que ver con dispositivos del IoT según Gartner

Un 48% de las empresas no son capaces de detectar si alguno de sus dispositivos de IoT se ha visto afectado por una violación de seguridad

(Gemalto The State of IoT Security 2018)

EL IMPACTO ECONÓMICO DEL CIBERCRIMEN

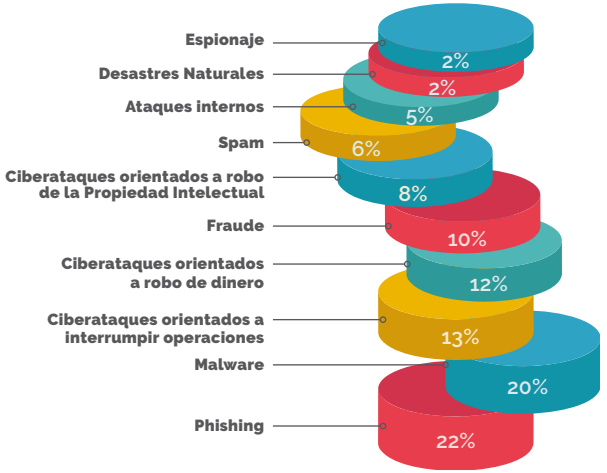
LOS 10 TIPOS DE INFORMACIÓN QUE MÁS VALORAN LOS CIBERCRIMINALES



Se estima que el coste de los ransomware llegue a más de 6 billones por año para el 2021 (Cybersecurity Ventures)

https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

LAS 10 PRINCIPALES AMENAZAS PARA LAS EMPRESAS



La razón principal por la que las empresas son atacadas tiene que ver con la obtención de información crítica de clientes o de la empresa.

Asimismo, uno de los ataques que más preocupan a los Responsables de Seguridad son los relacionados a ataques en sus sistemas con paradas de actividad, que sólo se recuperan si se paga un precio, lo que llamamos "Ransomware".

El Informe sobre ransomware 2020 llevado a cabo por el canal Datto revela, que éste sigue siendo la principal preocupación de las empresas, grandes y pequeñas de hecho, **dos de cada cinco pymes han sufrido un ataque de este tipo a lo largo de su existencia.**

MAERSK

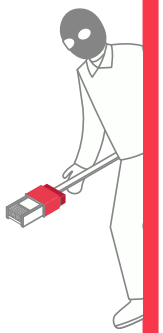
Un ataque que involucró al ransomware NotPetya costó a la empresa naviera Maersk más de 200 Millones

ISS

En 2020, un ataque de ransomware le costó a la empresa ISS con sede en Dinamarca más de 50 Millones €

Hydro

El fabricante de aluminio Norsk Hydro sufrió perdidas de más de 40 millones de dólares tan solo una semana después de que la variante Locker Goga causara interrupciones en sus fábricas



asco
EXCELLENCE IN AEROSTRUCTURES

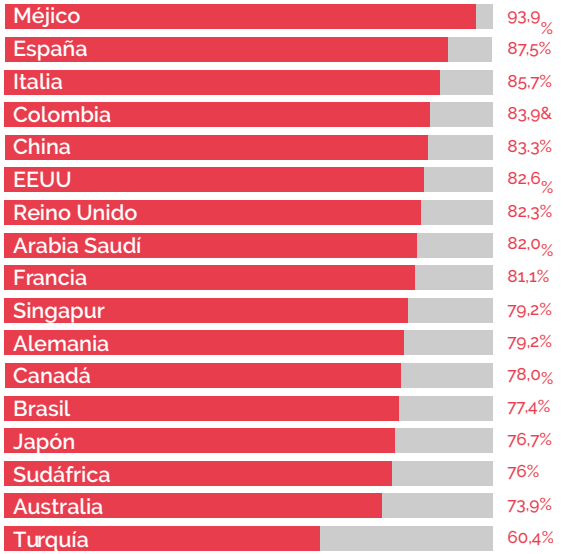
En el 2019 la empresa industrial belga, Asco, fabricante de componentes para la industria aeronáutica ufrió una interrupción grave en todas sus plantas en Bélgica, Alemania, Canadá y Estados Unidos, causada por un ataque

Adeslas
SegurCaixa

En 2020, SegurCaixa Adeslas sufrió un ataque ransomware que duró más de 6 semanas. Sus sistemas de informáticos y servicios digitales dejaron de funcionar de un día para otro

A nivel mundial México seguido de España fueron los países más afectado por ciberataques según el informe CyberEdge Group 2020 Cyberthreat Defense Report

Porcentaje del impacto de al menos un ataque, en los últimos 12 meses por país

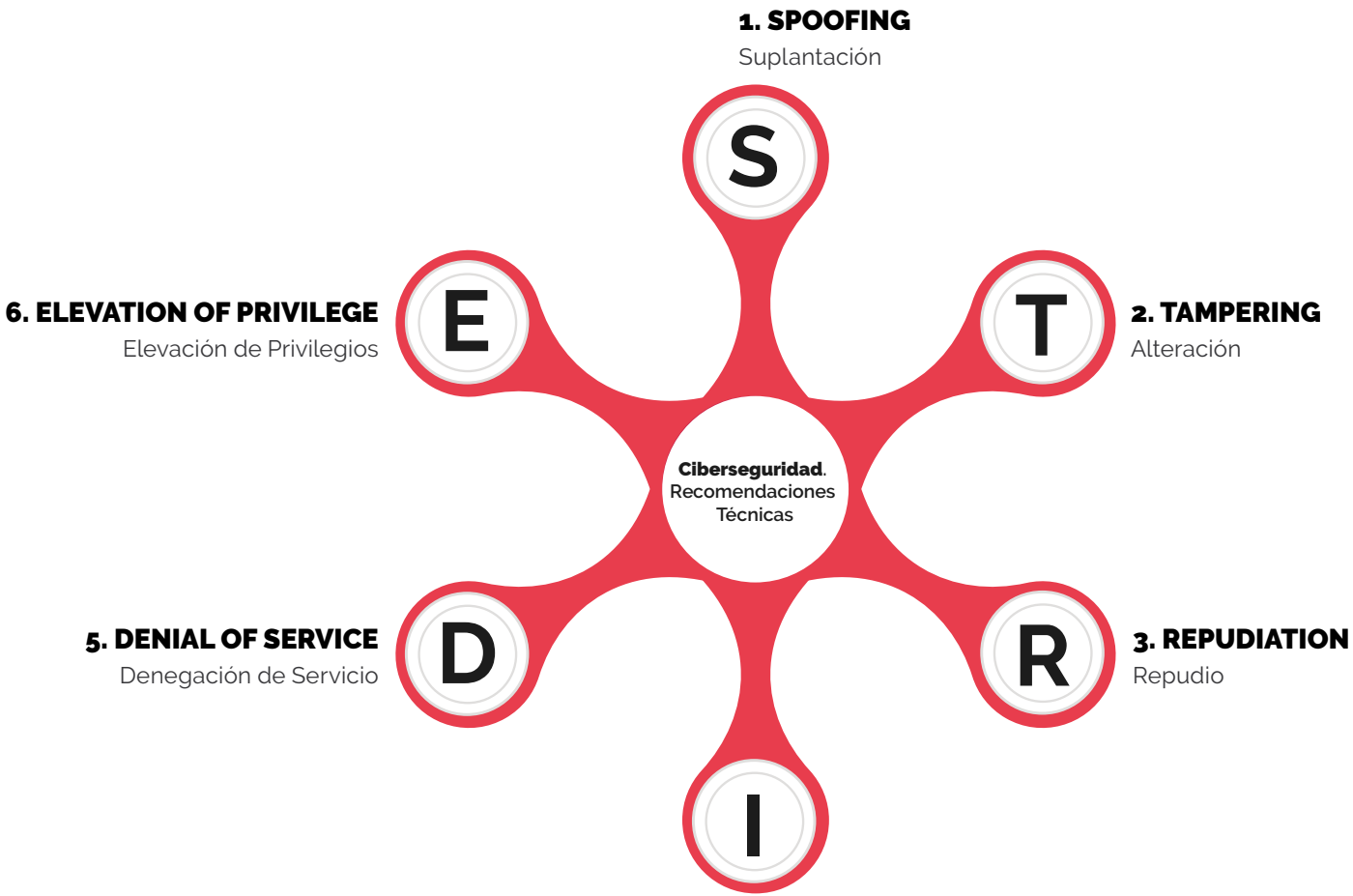


RECOMENDACIONES

RECOMENDACIONES TÉCNICAS

La metodología **STRIDE**, elaborada por Microsoft en 2000, es un mecanismo que ayuda a establecer un marco de análisis sobre las amenazas a controlar.

Este método clasifica las ciber-amenazas en 6 grandes grupos: Spoofing (Suplantación), Tampering (alteración), Repudiation (Repudio), Information Disclosure (Revelación de la Información), Denial of Service (Denegación del Servicio), Elevation of Privilege (Elevación de Privilegios).



SPOOFING
Suplantación

IMPACTO

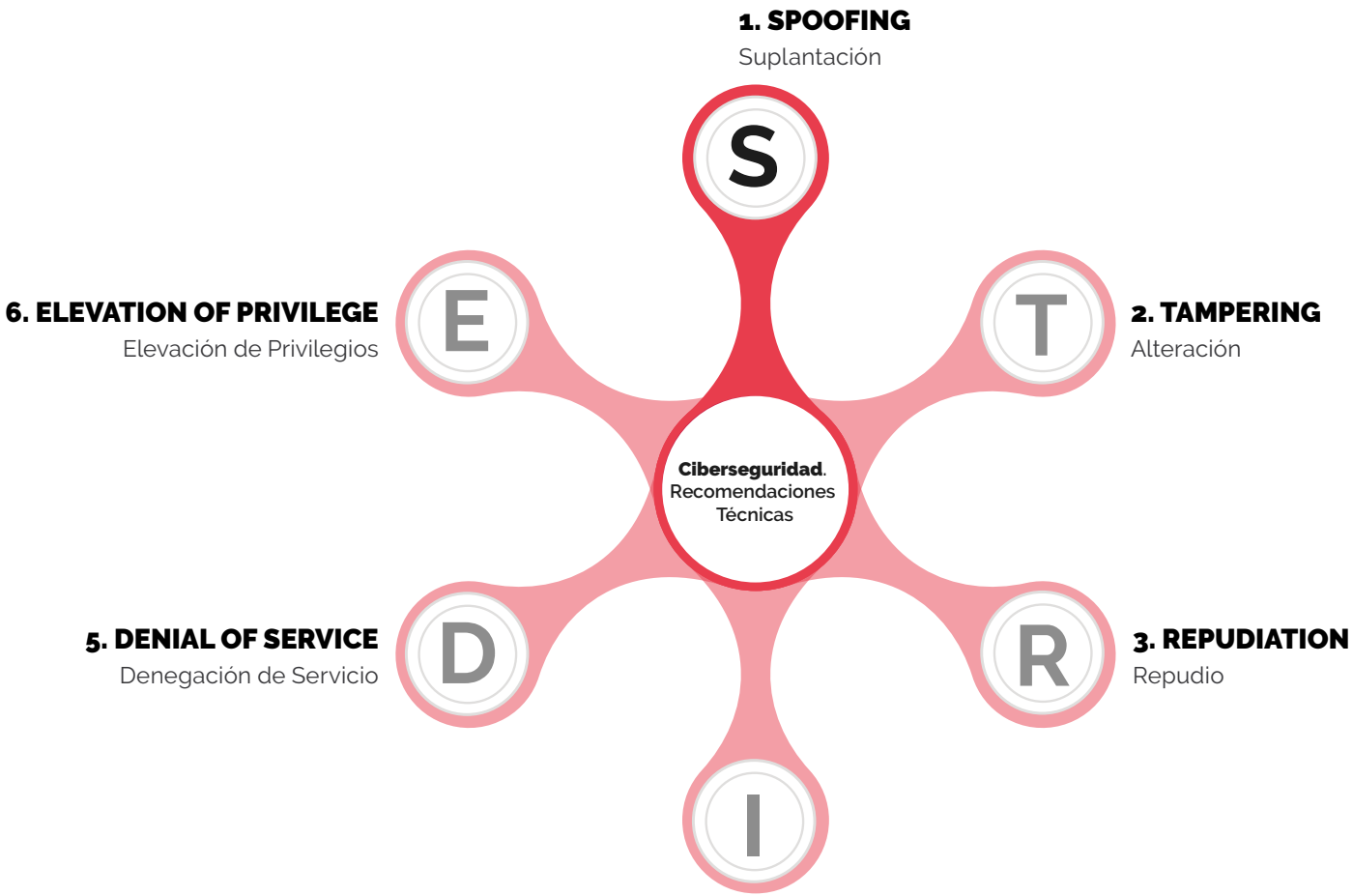
Engloban esta categoría los ataques orientados a suplantar la identidad de un usuario o sistema en la red.

En el IoT industrial, son especialmente relevantes los casos en los que un atacante puede hacerse pasar por un dispositivo y por tanto alterar el funcionamiento de las operaciones.

RECOMENDACIÓN

Para evitar estas amenazas es fundamental que los **sistemas de Autenticación** entre plataformas y dispositivos sean **robustos**.

Los usuarios y contraseñas se demuestran cada vez más inseguros, en favor de las autenticaciones mutuas (el dispositivo identifica a la plataforma, y la plataforma identifica al dispositivo) basadas en certificados digitales únicos.



TAMPERING
Alteración

IMPACTO

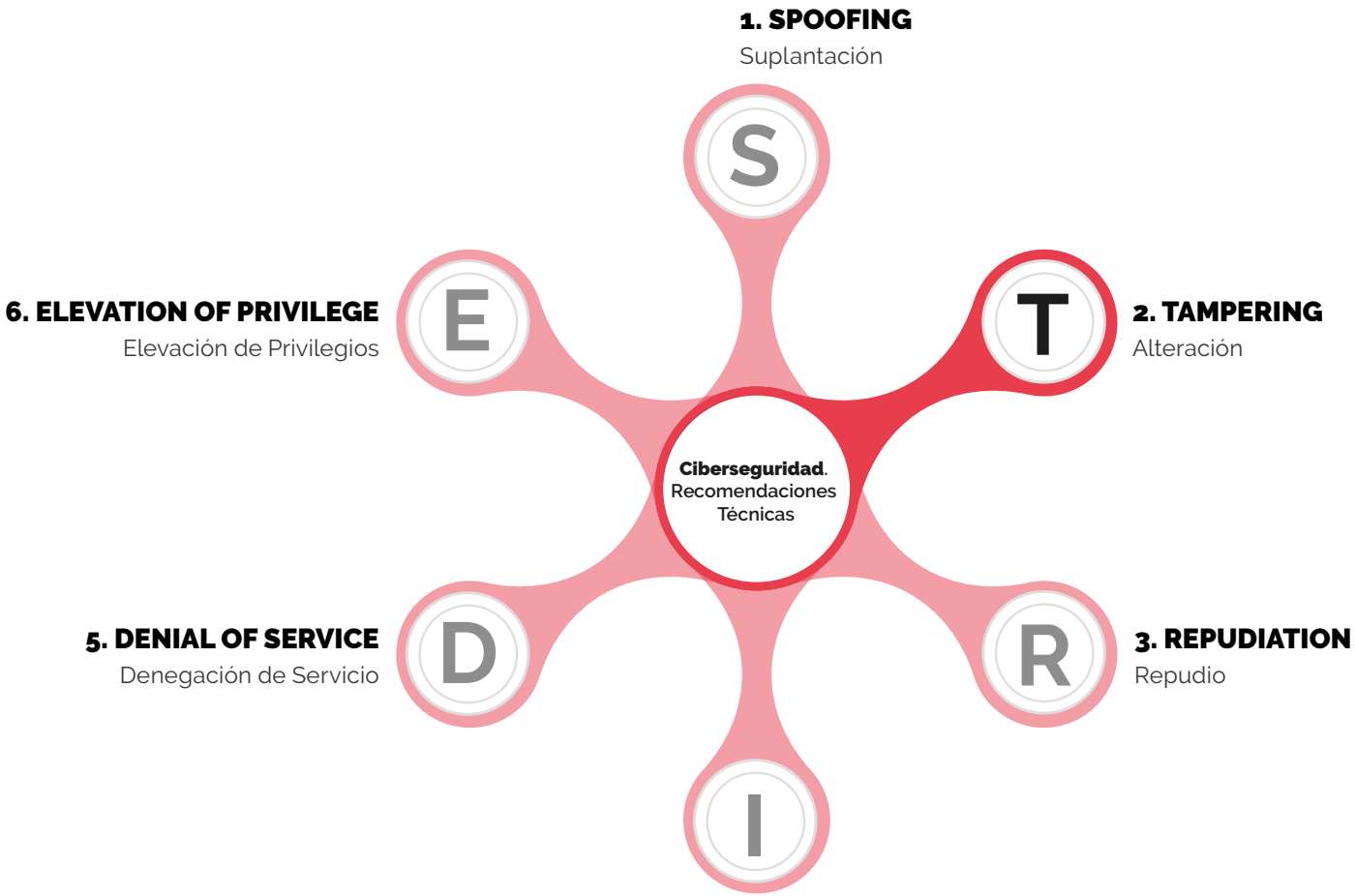
Son amenazas relacionadas con la posibilidad de que un dispositivo IoT sea alterado, y por tanto su funcionalidad cambiada.

Dado que algunos dispositivos conectados están ligados a la operación del negocio, la protección contra este tipo de ataques es crítica en la industria.

RECOMENDACIÓN

En este sentido, los **dispositivos con firmware seguro** y certificados de acuerdo a una norma como la IEC-62443-4 minimizan este riesgo.

Este tipo de dispositivos, elevan el nivel de seguridad y reducen dramáticamente la posibilidad de que un agente no deseado modifique su hardware o software para alterar su funcionamiento.



REPUDIATION
Repudio

IMPACTO

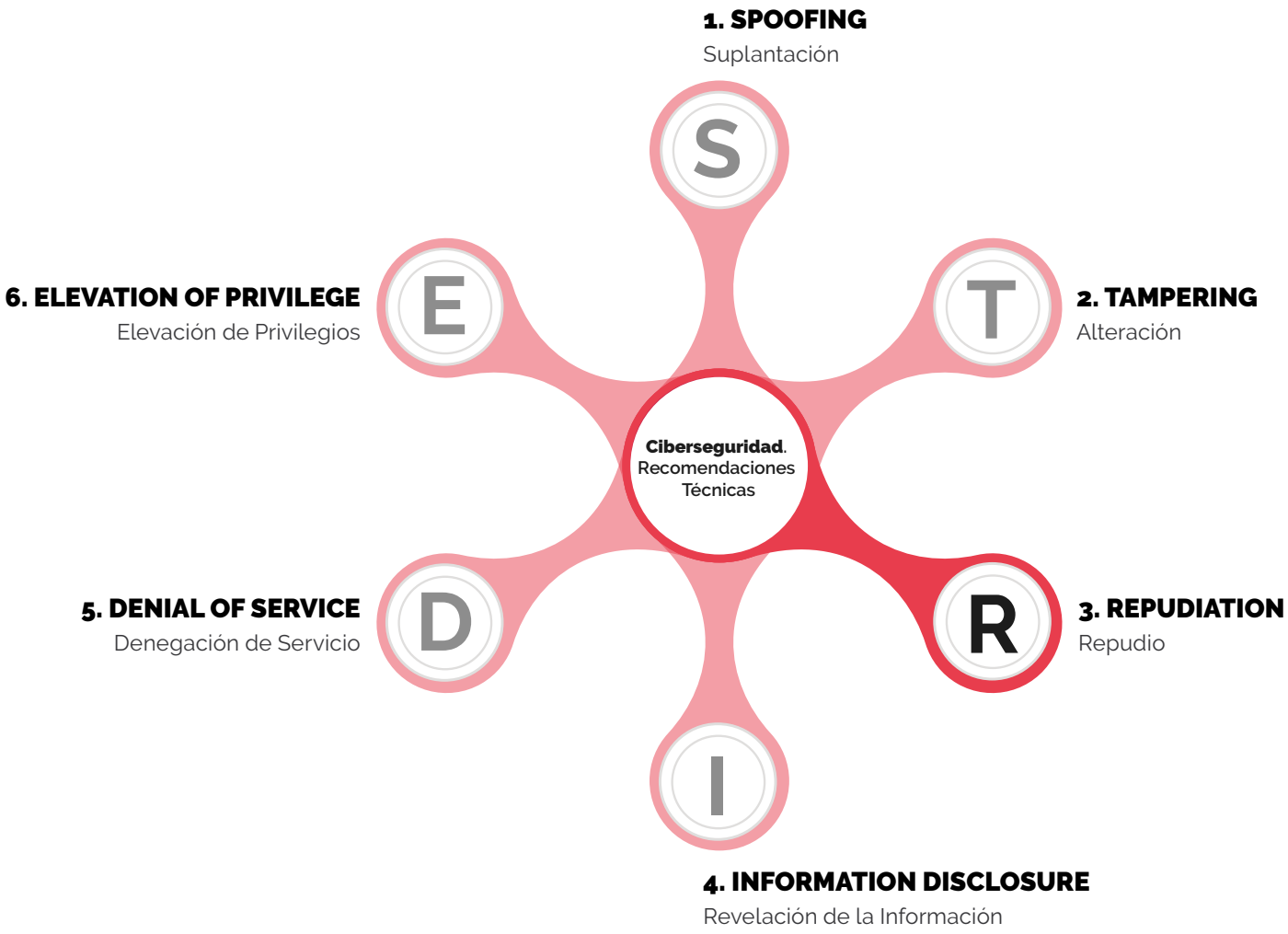
Este grupo incluye aquellos incidentes en los cuales se pueden realizar cambios en los sistemas cuyo originante pueda negar su autoría.

Este caso tiene especial relevancia en los escenarios en los que el atacante podría ser un "insider" (empleado de la compañía trabajando para la competencia).

RECOMENDACIÓN

En el IoT industrial los elementos más afectados por los riesgo de Repudio, son las platformas, dado que agrupan datos o gestión de dispositivos, que podrían ser masivamente alterados sin dejar constancia de ello.

Para minimizar estos riesgos es fundamental la **NO compartición de usuarios y contraseñas** de acceso, así como la trazabilidad y almacenado histórico de cualquier acceso y operación realizada en los sistemas.



INFORMATION DISCLOSURE
Revelación de la Información

IMPACTO

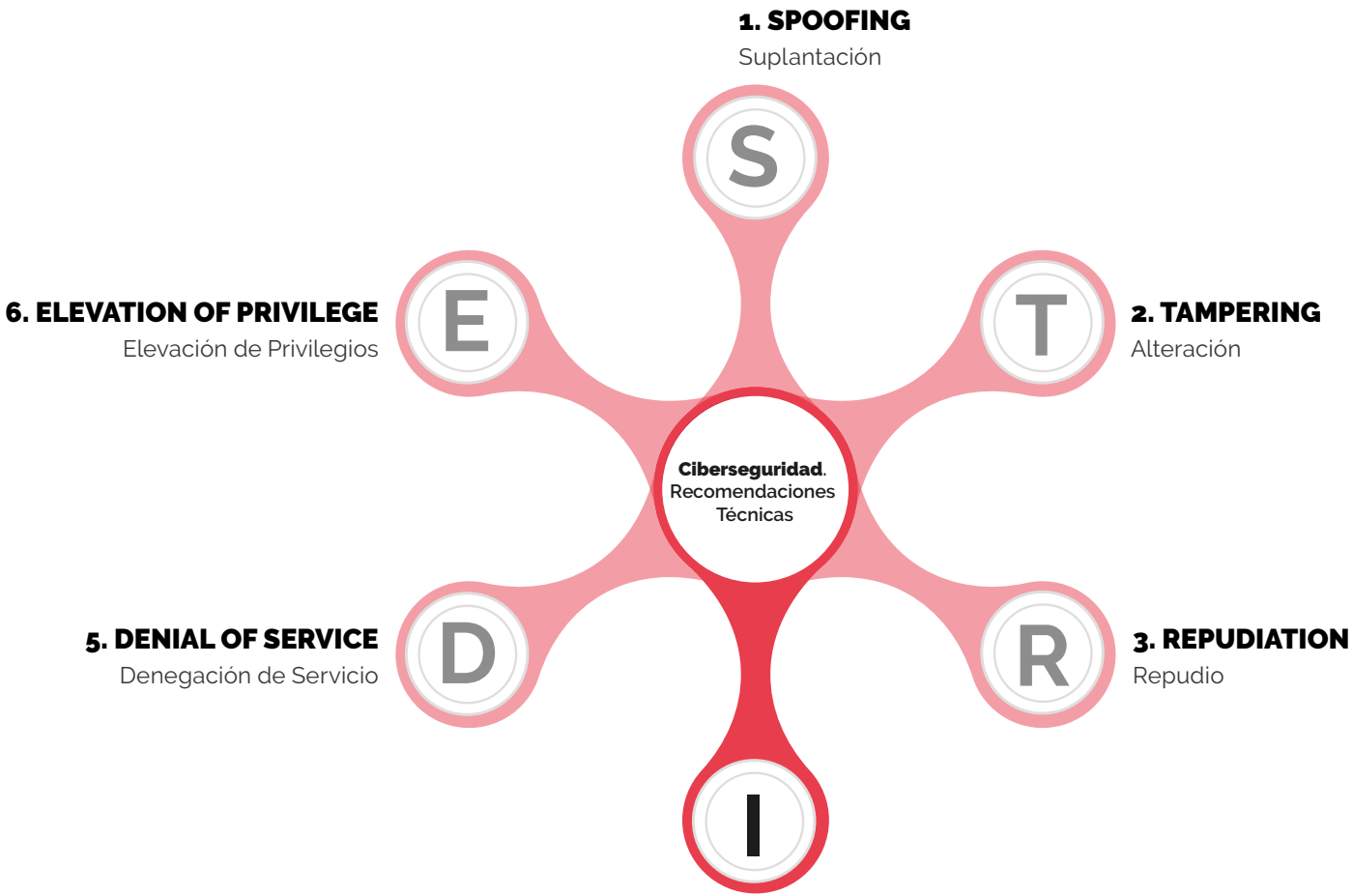
Incluye todos aquellos ataques orientados al robo de información confidencial, bien sea por espionaje industrial o para su venta o uso indebido.

Este escenario es relevante en el caso de IoT, dado que los dispositivos en muchos casos están desatendidos y pueden ser físicamente explorados, o incluso sustraídos, por un tercero. Las industrias con muchos activos conectados dispersos, como las utilities, estás especialmente expuestas a estos riesgos.

RECOMENDACIÓN

Es fundamental por tanto asegurar que la información digital en los dispositivos y en tránsito por la red, está encriptada siempre.

Si bien tecnologías estándar como AES-256 permiten un nivel de encriptación aceptable por la industria, la aparición de la computación cuántica, que permite desencriptar por prueba y error este tipo de algoritmos en tiempos reducidos, hacen imperativo comenzar a **evaluar sistemas que consideren la criptografía "post-cuántica".**



DENIAL OF SERVICE
Denegación de Servicio

IMPACTO

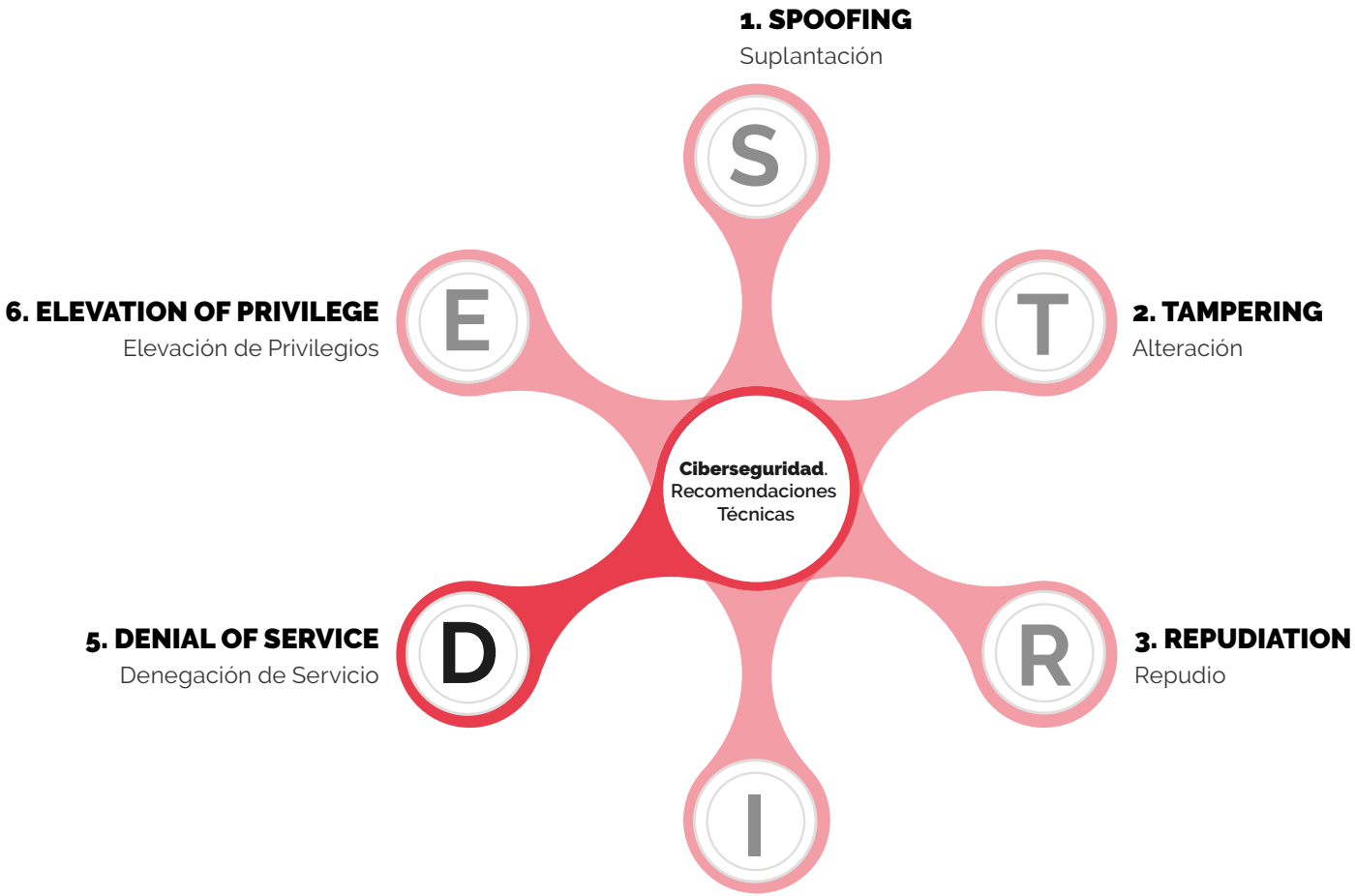
Es probablemente el riesgo más elevado al IoT industrial, dado que lo comúnmente conocido como ataques DoS son los que pueden llegar a parar la continuidad del negocio.

Dentro de esta categoría se encuadran los ataques de secuestro digital (Ransomware) que pueden para la operación de dispositivos y solicitar un rescata para la liberación de los mismo.

RECOMENDACIÓN

Para minimizar los riesgos de este tipo de ataques, las tecnologías de **segmentación de red** y los **sistemas de B&R** (Backup & Recovery), son imperativos en cualquier despliegue de IoT industrial. Si bien no afectan directamente a la capacidad que un atacante tenga para realizar un ataque DoS, si que reducen de manera muy directa el impacto que este puede tener.

La segmentación de red, impediría que el número de dispositivos involucrados en DoS solo se propagara a un segmento de red. Los sistemas de B&R permitirían que, cualquier dispositivo o sistema parado, pueda ser restaurado rápidamente a su estado anterior.



ELEVATION OF PRIVILEGE
Elevación de Privilegios

IMPACTO

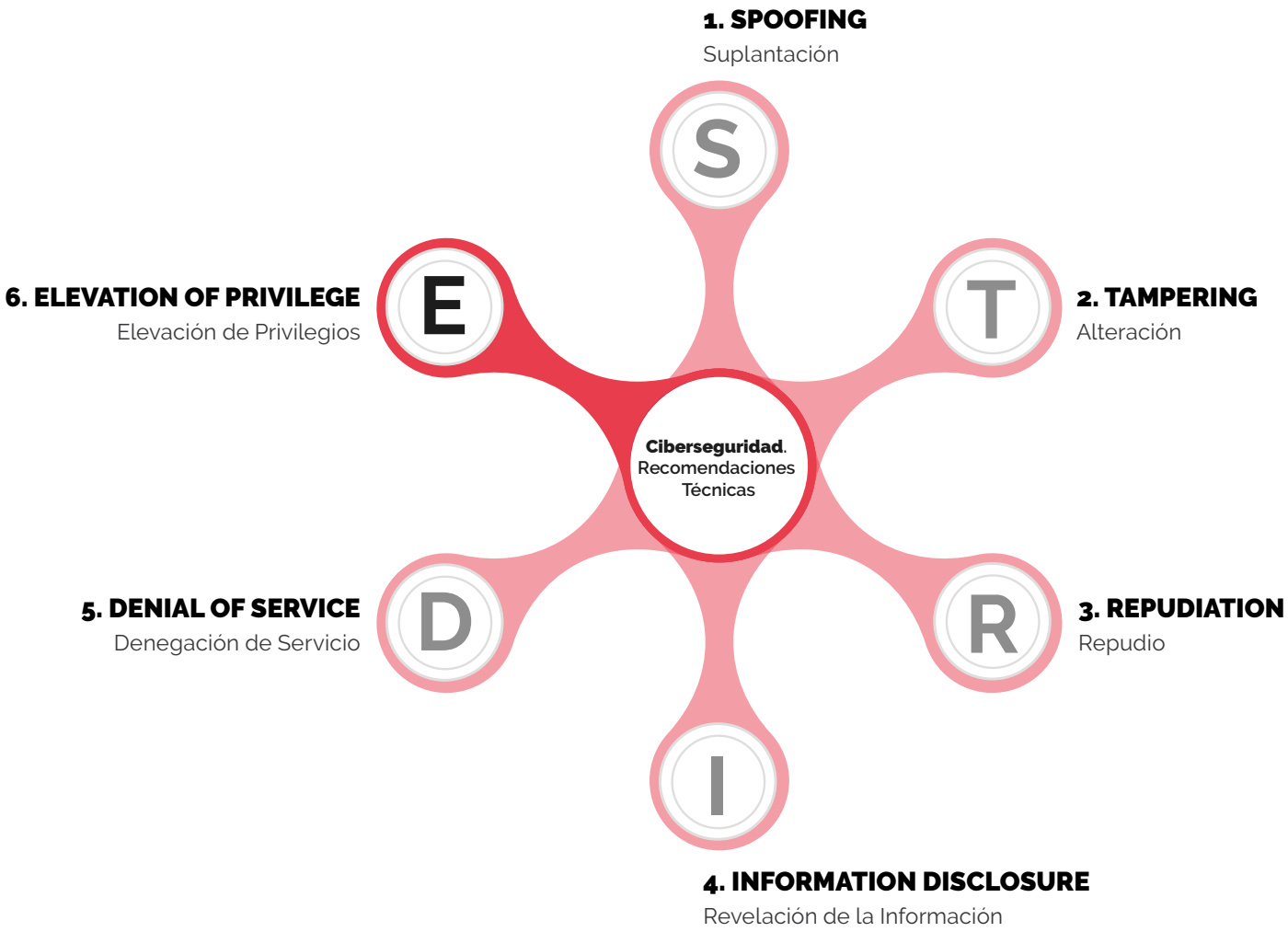
Contiene cualquier riesgo asociado a que un usuario a través de un sistema o dispositivo, pueda realizar acciones para las que inicialmente no debería tener permisos.

Por ejemplo, desde un sensor tiene sentido que se pueda escribir una base de datos en la nube, pero no que se pueda borrar la base de datos completa.

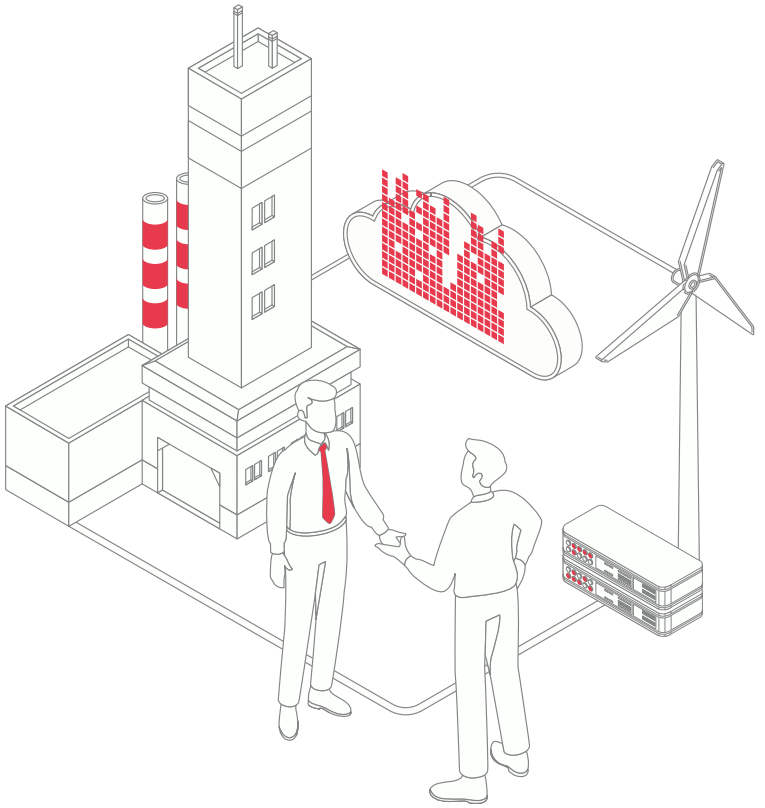
RECOMENDACIÓN

La escalación de privilegios viene normalmente causada por fallos de diseño, que en muchos casos se hacen públicos o semi públicos en forma de vulnerabilidades.

Para ello, disponer de herramientas que permitan la vigilancia tecnológica de vulnerabilidades, con las **herramientas de escaneo de activos o detección de intrusiones (IDS)**, se hacen vitales.



RECOMENDACIONES DE PROCESOS



Los procesos relacionados con la ciberseguridad son tanto o más importantes que las herramientas y tecnologías utilizadas. La combinación de unas buenas herramientas, con buenos procedimientos, es la clave en la minimización de los riesgos de ciberseguridad en el IoT industrial

El Framework de ciberseguridad para infraestructura críticas es una guía voluntaria, creada por el Instituto Nacional Americano de los estándares y la Tecnología (NIST), que identifica mediante un lenguaje común, cinco funciones orientadas a la reducción de riesgos de ciberseguridad en infraestructura crítica.

Las cinco funciones comprenden el núcleo del marco son identificar, proteger, detectar, responder y recuperar. Bajo estas funciones generales, el Framework proporciona una serie de pautas y prácticas existentes que las organizaciones pueden personalizar para administrar mejor su ciberseguridad.

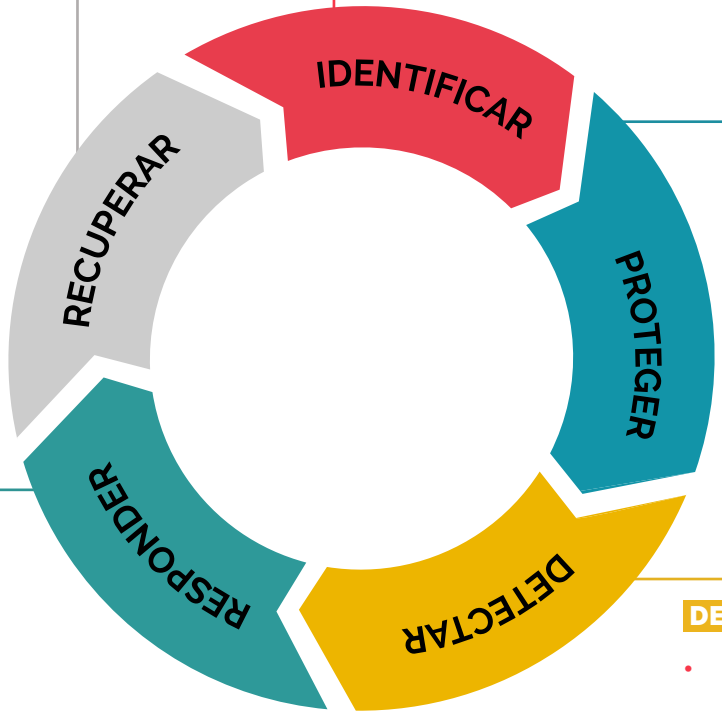
Disponiendo de las herramientas necesarias, es fundamental que las organizaciones industriales tengan un plan director, bajo el paraguas de un CISO (Chief Information Cibersecurity Officer) que especifique y documente los procesos que permitan en cada actividad optimizar los esfuerzos y resultados dedicados.

IDENTIFICAR

- Los escaneos periódicos de la red, en búsqueda de nuevos activos o superficies de ataques
- La auditoría periódica de ciberseguridad por parte de terceros de los entornos críticos IT y OT
- La vigilancia tecnológica en búsqueda de vulnerabilidades y tendencias del cibercrimen

RECUPERAR

- La capacidad de las actualizaciones remotas de software y firmware, y las ventanas periódicas para su realización
- La simulación periódica de escenarios de "Disaster Recovery"
- La formación técnica interna en los equipos críticos de terceros



PROTEGER

- La formación a los empleados, con cursos dedicados y herramientas de concienciación
- La inclusión de ciberseguridad en los procesos de RFP/RFQ de proveedores
- La aplicación sistemática de parches de seguridad

RESPONDER

- La disposición de un plan de respuesta a incidencias que incluya comunicación interna y externa
- La preparación de un plan de continuidad del negocio ante un ciberataque
- La disposición de asesoría legal especializada

DETECTAR

- La generación de reportes periódicos frecuentes
- Las alianzas con empresas de servicios gestionados de seguridad (MSSP)
- La elaboración de procesos de escalado de incidencias

RECOMENDACIONES DE PRESUPUESTOS

"De acuerdo a estándares recientes, las organizaciones dedican un 10% del presupuesto de IT a ciberseguridad"

Toda la información anterior sobre recomendaciones técnicas y de procesos, plantea la gran disyuntiva sobre cómo asignar y distribuir el presupuesto destinado a ciberseguridad.

Este % puede variar en función del tipo de mercado, siendo mayor en industrias más reguladas e infraestructuras críticas, como la energía o farmacéutica, y menor en industrias menos reguladas como la logística o manufactura. Un informe de **BCG (Boston Consulting Group) detectó una variabilidad de hasta 300% en los presupuestos asignados a ciberseguridad, lo que muestra, que lamentablemente en muchos casos el presupuesto asignado puede ser bajo**, o incluso nulo y completamente diluido en los grandes presupuestos de IT.

En cualquier caso, sí que se demuestra la tendencia de que la gestión de este presupuesto, que normalmente cae dentro del cargo del CISO, está cada vez más presente en la agenda ejecutiva de la compañía.

"Los CISOs van estando cada vez más cerca tan cerca del CEO, como lo estaban tradicionalmente del CTOs"

El ROI de un presupuesto asociado a ciberseguridad debe poder ser medido con KPIs que aseguren su funcionamiento, y en este sentido el valor de esta inversión tiene que ser medido contra la capacidad de la empresa para tener un nivel de riesgo bajo, y permanecer conforme a normas de ciberseguridad industrial a las que se haya acogido. En ese sentido, más allá de los KPIs obvios sobre el número de incidentes o los tiempos de respuesta a los mismos, invitar a terceras partes a realizar auditorías de ciberseguridad y tests de penetración en los activos de la empresa ayudará a validar la eficiencia del presupuesto de manera más continua.

ESTANDARIZACIÓN Y NORMATIVA

ESTÁNDARES MÁS DESTACADOS

Varios organismos recogen requisitos y recomendaciones relativas a la ciberseguridad para IoT que se traducen en varios estándares y guías de implementación.

IEC 62443

Este estándar está enfocado al **ámbito de la Industria 4.0.** Es en realidad un conjunto de estándares que ofrece un acercamiento a la ciberseguridad industrial a lo largo de todo el ciclo de vida de un proyecto: desde la auditoría de riesgos hasta las operaciones. Busca reducir los riesgos que puedan afectar a los activos en entornos industriales.

Estos estándares están clasificados en 4 bloques:

- **General:** recogen conceptos fundamentales, modelos de referencia y terminología
- **Políticas y procedimientos:** en ellos se orienta en la construcción de un programa de gestión de ciberseguridad
- **Sistema:** engloba tecnologías de protección y requisitos para lograr un nivel de seguridad determinado
- **Componentes:** Requisitos técnicos de ciberseguridad en el ciclo de vida de desarrollo de productos

IIC - IISF

OWASP – IOT PROJECT

GSMA

IOT SECURITY COMPLIANCE FRAMEWORK

IEC 62443 | **IIC - IISF** | OWASP – IOT PROJECT | GSMA | IOT SECURITY COMPLIANCE FRAMEWORK

El propósito del Industrial Internet of Things, Volumen G4: Marco de seguridad (IISF) desarrollado por el Industrial Internet Consortium (IIC) es identificar, **explicar y posicionar arquitecturas, diseños y tecnologías** relacionadas con la seguridad, así como identificar **procedimientos relevantes para la confiabilidad** de los sistemas del Internet industrial de las cosas (IIoT).

Un sistema IoT exhibe características de extremo a extremo que surgen como resultado de las propiedades de sus diversos componentes y la naturaleza de sus interacciones. Las **cinco características que más afectan las decisiones de confianza** de una implementación de IIoT son:

- Seguridad - Security
- Seguridad – Safety
- Fiabilidad
- Resiliencia
- Privacidad

No hay esquema de evaluación. Sin embargo, la el IIC tiene bancos de pruebas en cinco mercados diferentes: energía, salud, manufactura, ciudades inteligentes y transporte. Los bancos de pruebas son dónde la innovación y las oportunidades de Internet industrial (nuevas tecnologías, nuevas aplicaciones, nuevos productos, nuevos servicios, nuevos procesos) pueden iniciarse, meditarse y probarse rigurosamente para determinar su utilidad y viabilidad antes de salir al mercado.

IEC 62443 | IIC - IISF | **OWASP – IOT PROJECT** | GSMA | IOT SECURITY COMPLIANCE FRAMEWORK

El proyecto de IoT de OWASP está diseñado para **ayudar a los fabricantes, desarrolladores y consumidores a comprender mejor los problemas de seguridad asociados con Internet de las cosas**, y para permitir a los usuarios en cualquier contexto tomar mejores decisiones de seguridad al construir, implementar o evaluar tecnologías de IoT.

Define un conjunto de áreas específicas para los dispositivos IoT y sus vulnerabilidades relacionadas, como por ejemplo:

- Interfaces físicas del dispositivo
- Interfaz web del dispositivo
- Firmware del dispositivo
- Servicios de red de dispositivos
- Interfaz administrativa
- Almacenamiento local de datos
- API de backend de terceros
- Mecanismo de actualización
- Autorización de autenticación
- Privacidad

...entre otras.

Los puntos más críticos que este marco resalta y que son la causa de las vulnerabilidades más graves incluyen aspectos como:

- Falta de mecanismo de actualización segura
- Uso de componentes inseguros u obsoletos
- Protección de privacidad insuficiente
- Transferencia y almacenamiento de datos inseguros
- Falta de un sistema de gestión de dispositivos
- Uso de contraseñas débiles, adivinables o codificadas
- Existencia de interfaces inseguras en el ecosistema, ya sea web, API de back-end, nube o interfaces móviles en el ecosistema

IEC 62443 | IIC - IISF | OWASP – IOT PROJECT | GSMA | IOT SECURITY COMPLIANCE FRAMEWORK

Las Pautas de seguridad de IoT creadas por la GSMA promueven una metodología para desarrollar servicios de IoT seguros. Las recomendaciones se presentan con diferentes grados de criticidad y se centran en dos componentes de IoT: Ecosistema de "Endpoint" y Ecosistema de Servicio.

El **ecosistema de "Endpoint"** se incluye a dispositivos de baja complejidad, dispositivos avanzados y puertas de enlace ("gateways") que conectan el mundo físico con el mundo digital a través de varios tipos de redes cableadas e inalámbricas.

Las recomendaciones catalogadas con la mayor criticidad para estos sistemas incluyen aspectos como:

- Implementar una base de cómputo de confianza de Endpoint
- Utilizar un ''Tamper Resistant Trust Anchor''
- Aprovisionar de forma exclusiva cada punto final
- Realizar una gestión de contraseñas de punto final
- Usar un generador de números aleatorios comprobados
- Firmar criptográficamente imágenes de aplicaciones
- Hacer cumplir la protección de la memoria
- Realizar la carga de arranque fuera de la ROM interna
- Bloquear secciones críticas de la memoria

...entre otros

El **ecosistema de servicios** representa el conjunto de servicios, plataformas, protocolos y otras tecnologías necesarias para proporcionar capacidades y recopilar datos de puntos finales implementados en el campo.

Las recomendaciones que dentro de este ecosistema se consideran más críticas incluyen :

- Definir una infraestructura de seguridad para los sistemas expuestos a la Internet pública
- Definir un enfoque de registro y monitoreo de sistema.
- Definir un modelo de respuesta a incidentes
- Definir un modelo de recuperación

...entre otras.

IEC 62443 | IIC - IISF | OWASP – IOT PROJECT | GSMA | **IOT SECURITY COMPLIANCE FRAMEWORK**

Creado por la IoT Security Foundation, es una **lista de verificación** para guiar a una compañía a través del proceso de aseguramiento y reunir evidencia estructurada para demostrar el cumplimiento de las mejores prácticas. Al ser un documento de buenas prácticas, no consta de un esquema de certificación asociado. No obstante, incluye un exhaustivo cuestionario basado en estas buenas prácticas que permite evaluar su grado de cumplimiento.

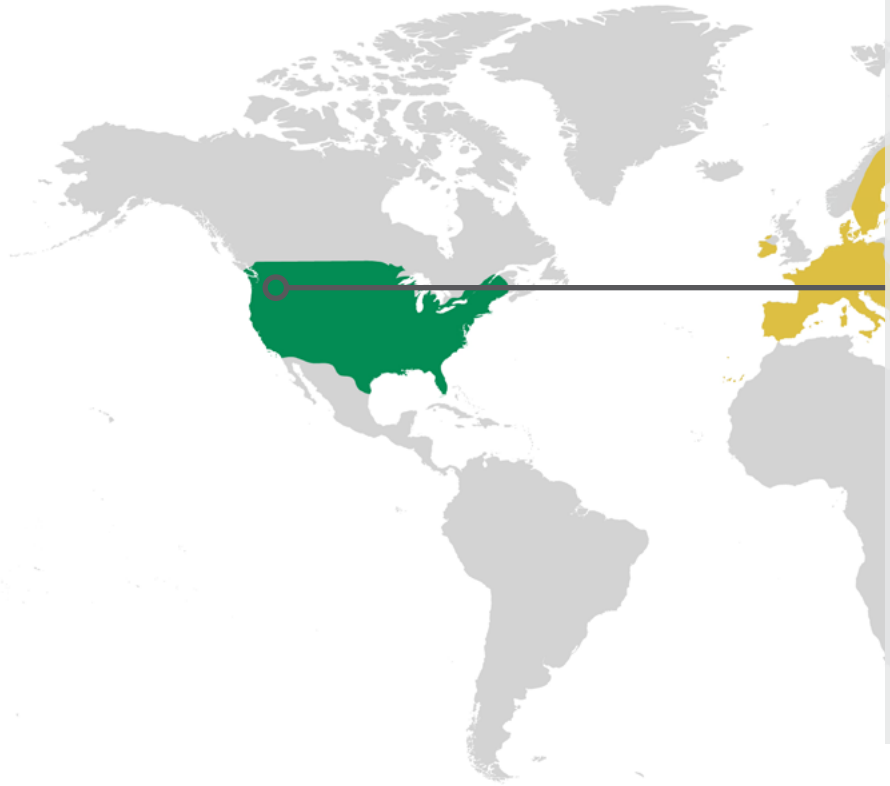
Estas **buenas prácticas** cubren aspectos como:

- Procesos de seguridad empresarial y responsabilidad
- Hardware de los dispositivos y seguridad física
- Sistema operativo de los dispositivos
- Aplicaciones software sobre los dispositivos
- Interfaces (cableadas o inalámbricas) de acceso al dispositivo
- Autenticación y Autorización
- Nube y elementos de red
- Cadena de suministro y producción
- Configuración

...entre otros.

REGULACIÓN

A nivel regulatorio, merece la pena destacar las iniciativas que se están llevando a cabo en Estados Unidos, la Unión Europea y Australia

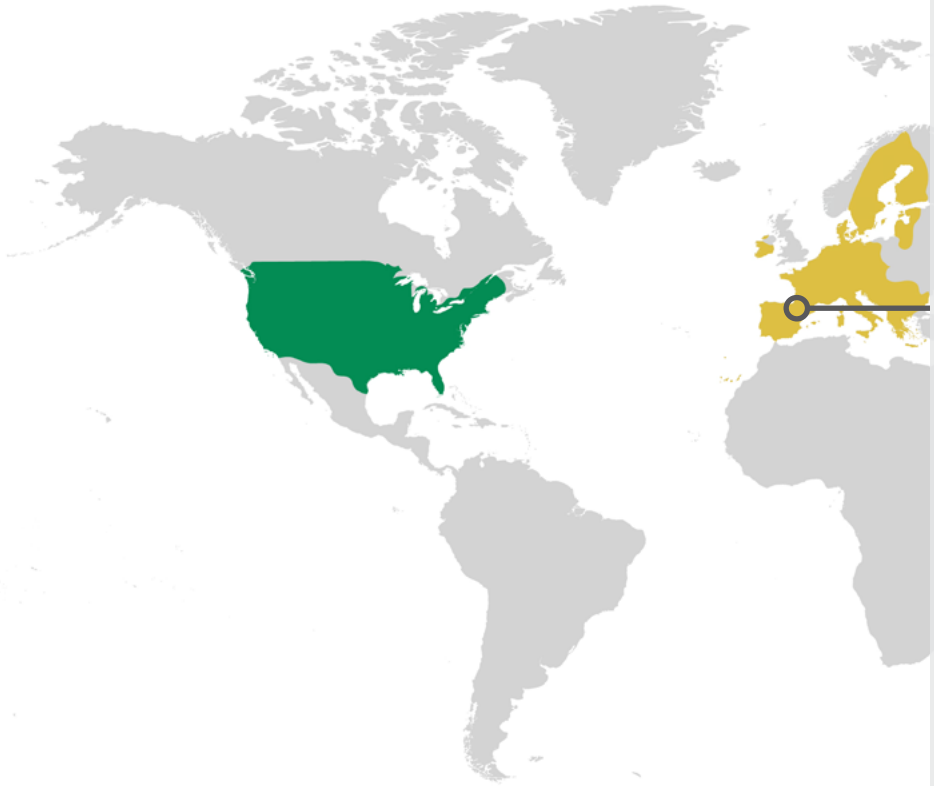


ESTADOS UNIDOS

La IOT CYBERSECURITY IMPROVEMENT ACT insta a la instituto nacional estadounidense de estandarización y tecnología (NIST) a definir un marco de requisitos en el ámbito de la ciberseguridad IoT que será **de obligado cumplimiento para los productos que cualquier agencia federal decida adquirir** y que debe cubrir al menos aspectos como:

- la seguridad del código
- la administración de identidades
- la política de parcheo
- la administración de la configuración

A nivel estatal, California y Oregon cuentan ya con leyes en vigor que regulan aspectos relacionados con la ciberseguridad en IoT. Se centra en los dispositivos físicos, prohibiendo la venta de aquellos que no tengan una base de seguridad razonable.



UNION EUROPEA

No cuenta aún con un Reglamento o una Directiva (los actos legislativos más parecidos al concepto de 'ley' que la UE puede aprobar) que regule la ciberseguridad en el ámbito del IoT.

No obstante, y aunque una regulación específica para IoT evitará cualquier duda, ya la **"Regulation 2019/881 on ENISA and ICT Cybersecurity Certification"** establece un marco para el establecimiento de una certificación de ciberseguridad europea para productos, servicios y procesos ICT (de las Tecnologías de la Información y la Comunicación por sus siglas en inglés). **Esta regulación afectaría,** pues, tanto **a dispositivos como infraestructuras del IoT** ya que, de acuerdo a la definición que la propia regulación establece en el Artículo 2 sobre qué es un producto, servicio o proceso ICT engloba cualquier dispositivo o servicio que recoja, envíe u opere datos. Además, esta regulación específicamente menciona la problemática de la seguridad en IoT en varias partes del texto, lo que confirma la consideración de categoría ICT a estos productos.

También destacan los esfuerzos realizados por la **Agencia de la Unión Europea para la Ciberseguridad (ENISA)**, que ha desarrollado exhaustivos manuales con guías y recomendaciones que se deben implementar en IoT para asegurar la integridad de los equipos y los datos como, por ejemplo el documento Guidelines for Securing the Internet of Things.

AUSTRALIA

Ha lanzado un **código de práctica voluntario para la securización del IoT** cuya intención es proporcionar a la industria de una guía de buenas prácticas sobre cómo diseñar dispositivos IoT con funcionalidades de ciberseguridad.

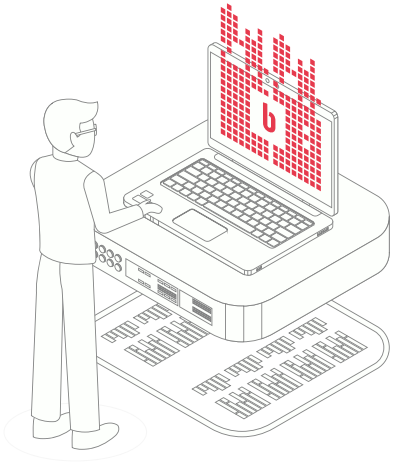
Aplicará a todos los dispositivos IoT de consumidor final **(no está pensado para el IoT Industrial)** que se conecten a internet para enviar o recibir datos en Australia, incluyendo "dispositivos del día a día como frigoríficos inteligentes, televisores inteligentes, monitores de bebé y cámaras de seguridad". Busca fomentar el desarrollo de los dispositivos IoT con una filosofía de Seguridad desde el diseño ("Security by design").

Este código se basa en 13 principios, entre los cuáles son especialmente relevantes los 2 siguientes:

- Implementar una política de notificación de vulnerabilidades que incluya un punto de contacto público para que investigadores de seguridad y otros puedan reportar cualquier incidencia de ciberseguridad
- Mantener el software actualizado de manera segura

NUESTRA VISIÓN PARA UN IOT INDUSTRIAL SEGURO

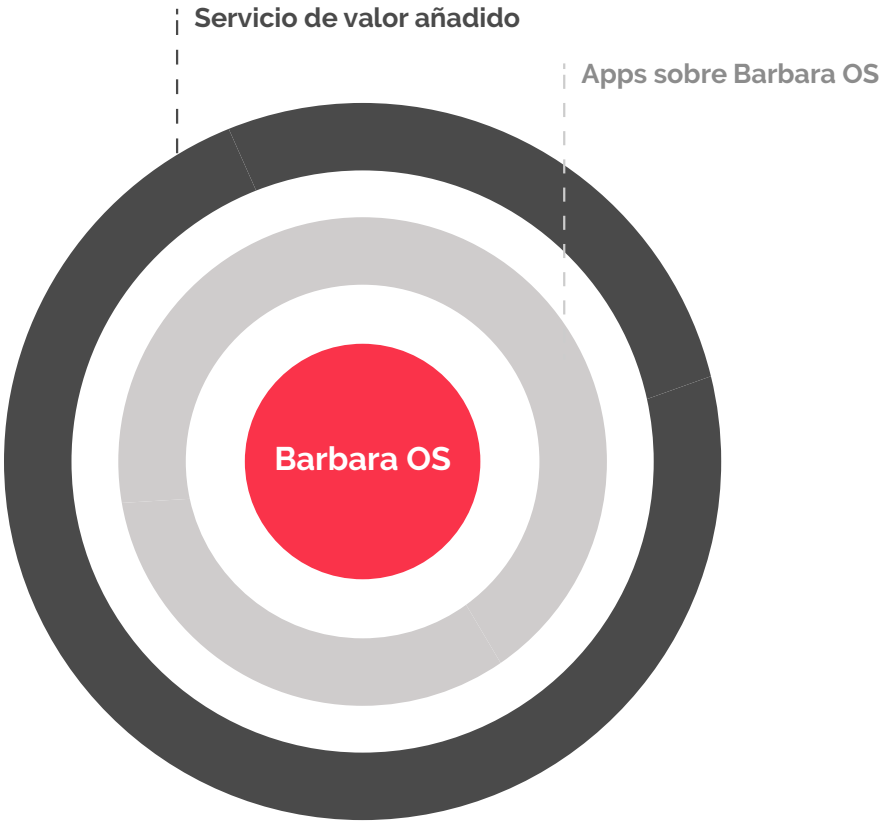
LA SEGURIDAD DESDE EL DISEÑO



Salvaguardar la integridad de los datos y de las máquinas sólo es posible cuando se incorpora la ciberseguridad desde dentro

En Barbara IoT tenemos como **misión securizar los dispositivos del IoT Industrial y facilitar su despliegue a gran escala**, a través de su software seguro. Un software que ha sido concebido con la seguridad como principal guía de diseño y que se ha incorporado desde las fases tempranas del desarrollo del software.

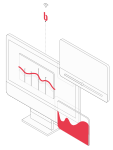
La seguridad por diseño es, más que una técnica de desarrollo, un concepto de la Ingeniería de Software y como tal, hemos creado un software que da respuesta a requisitos críticos de privacidad y de resiliencia, tan importantes para la Industria 4.0.



NUESTRO ACERCAMIENTO A LA SEGURIDAD

1. Gestión de Certificados por dispositivo

Barbara OS utiliza un control de identidad y de acceso al servicio cloud basado en certificados criptográficos por dispositivo. Esto se hace de manera transparente al usuario final y es gestionable remotamente a través de nuestra solución de gestión remota del ciclo de vida de los dispositivos



2. Sistema de monitorización y autocorrección

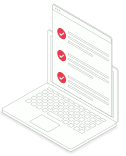
A través de su sistema activo de monitorización, Barbara OS permite reducir el tiempo de parada de un dispositivo por fallo, permitiendo corregir de forma autónoma y automática los problemas de sistema.

3. Encriptación completa de todos los datos

Tanto los datos de sistema como los de usuario en Barbara OS están encriptados en reposo (es decir, incluso cuando el dispositivo no está en uso). De esta forma, se previene la extracción de datos sensibles del dispositivo por parte de una entidad no autorizada o un atacante malicioso. Asimismo, Barbara OS implementa protocolos de seguridad estándar para la capa de transporte, como TLS y DTLS en sus versiones más restrictivas.

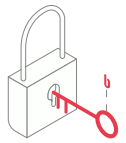
4. Gestión de Permisos de usuario

Barbara OS segmenta de manera muy clara el acceso a los datos de aplicaciones de usuario que corran en el dispositivo, y previene el riesgo producido por un escalado en los privilegios.



5. Gestión de Errores

Barbara OS implementa un completo sistema de traceo que permite detectar potenciales eventos relacionados con la seguridad o problemas funcionales y que se integra fácilmente con soluciones SIEM.



6. Integridad del Sistema

Mediante la ejecución de algoritmos criptográficos de chequeo durante el arranque, Barbara OS es capaz de determinar si un software a ejecutar ha sido correctamente firmado con las claves criptográficas adecuadas. De esta manera, se garantiza que el origen de esta porción de software es conocido, confiable y no ha sido alterado.

REFERENCIAS EXTERNAS

- Especificación Técnica IEC/TS 62443-1-1 , IEC
- Regulation of Internet-of-Things cybersecurity in Europe and Germany as exemplified by devices for children, por Stefan Hessel y Andreas Rebmann, Springer
- Regulation (EU) 2019/ of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cyb, Parlamento Europeo
- Code of Practice, Securing the Internet of Things for Consumers , Gobierno de Australia
- NISTIR 8259, Foundational Cybersecurity Activities IoT Device Manufacturers, Instituto Nacional americano de Estándares y Tecnología
- Senate Passes IoT Cybersecurity Improvement Act, por Jeremy Kirk
- Bill Text - SB-327 Information privacy: connected devices. Parlamento de California
- House Bill 2395, Parlamento de Oregón
- Research & Innovation in Internet of Things - Shaping Europe's digital future, Programas de I+D de la Unión Europea
- Mejorando la seguridad de la internet de las cosas…, por Enrique Dans
- Industrial Internet of Things Volume G4: Security Framework, Industrial Internet Consortium
- OWASP Internet of Things Project, OWASP
- IoT Security | Internet of Things, GSMA
- OTA IoT Trust Framework, Internet Society
- 27 Feb Global Ransomware Damage Costs Predicted To Exceed $5 Billion In 2017, por Steve Morgan
- 300+ Terrifying Cybercrime & Cybersecurity Statistics, por Andra Zaharia
- Guidelines for Securing the Internet of Things, ENISA

barbara

Para estar informado sobre IoT industrial y ciberseguridad, suscríbete a nuestra newsletter

2020 | info@barbaraiot.com | www.barbaraiot.com