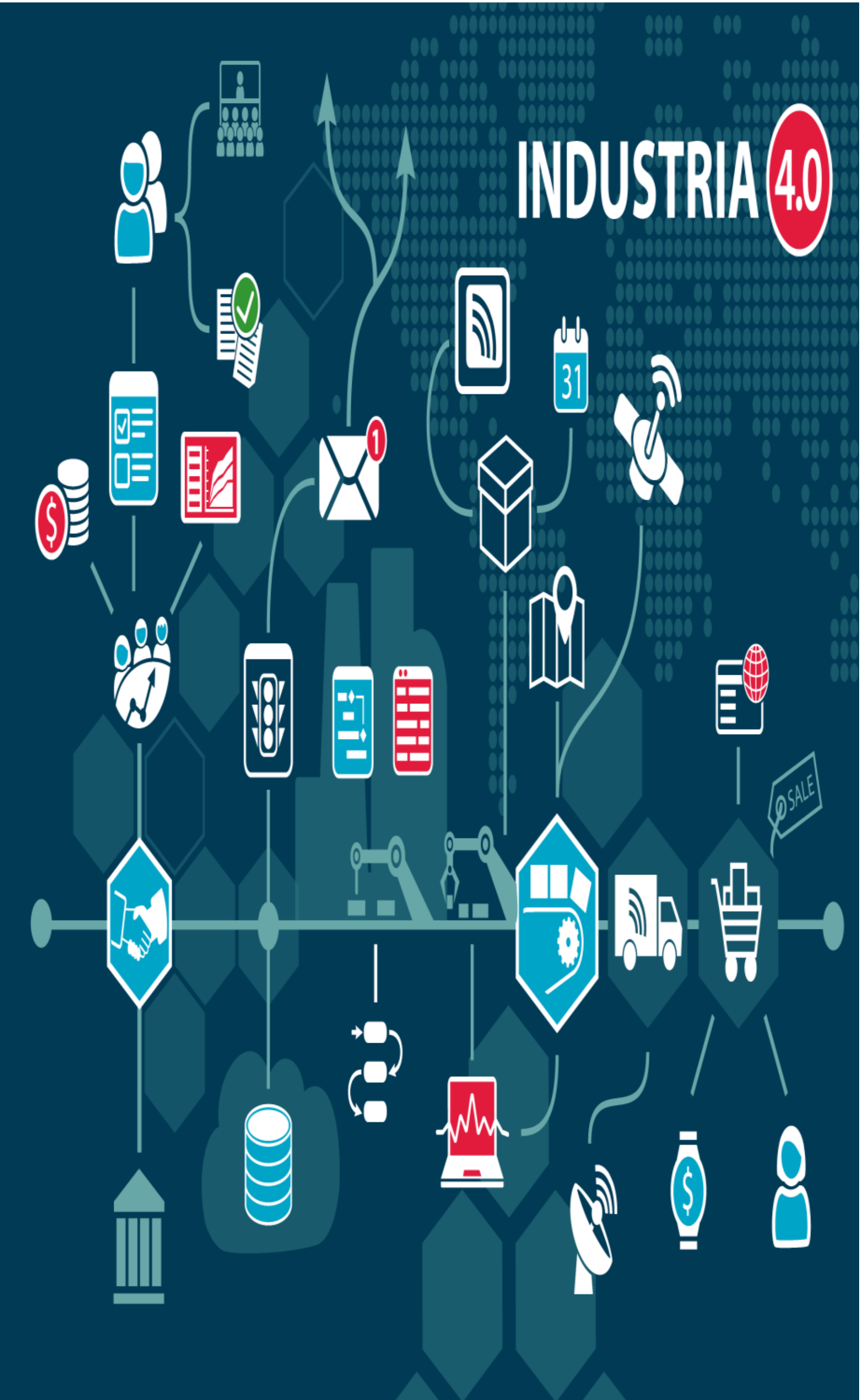
Superando barreras de la ciberseguridad

Joserra Concha García

Joserra.concha@pers.eus

Superando barreras de gestión durante la transformación digital

Índice



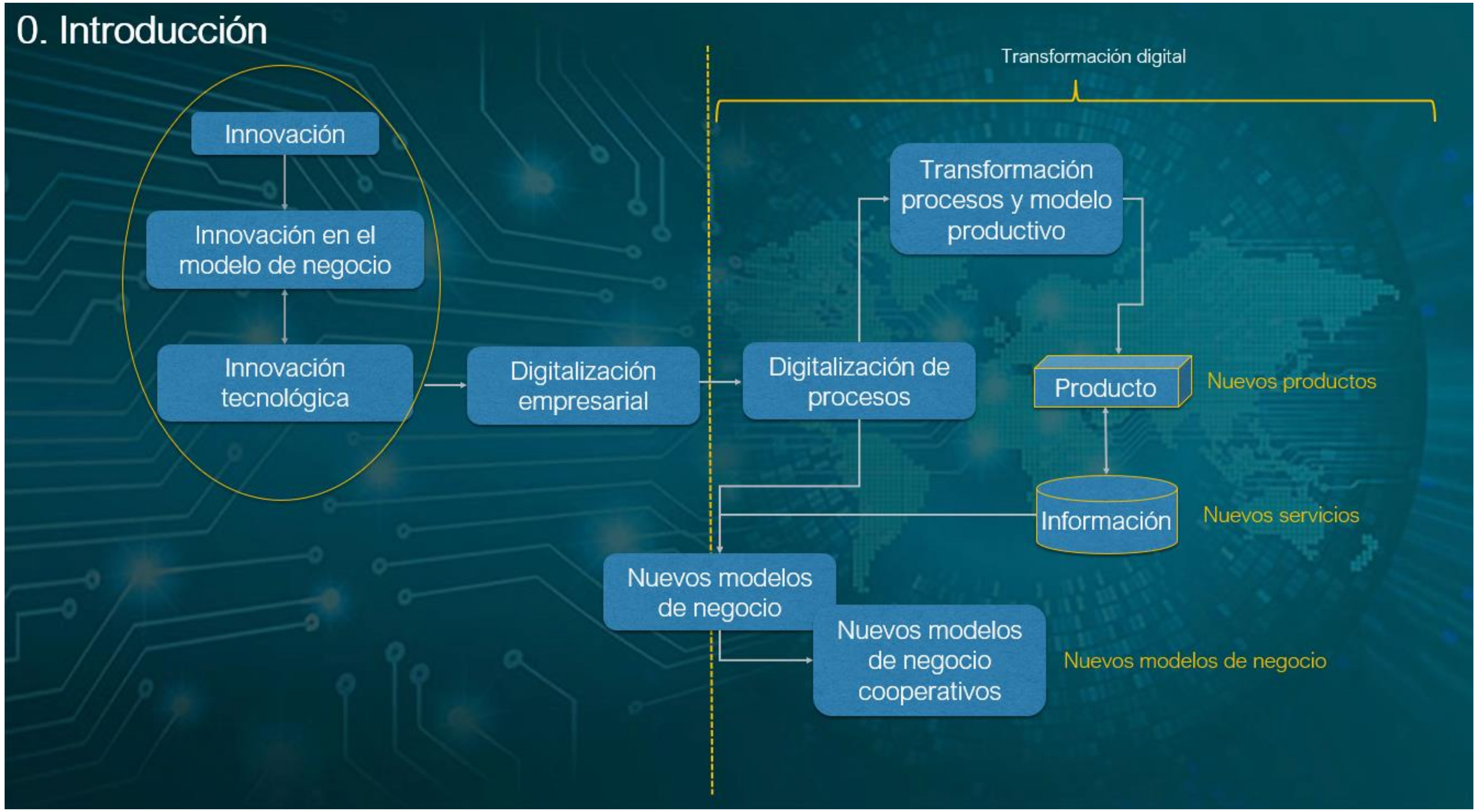
¿Qué es una “Organización Digital Segura”?

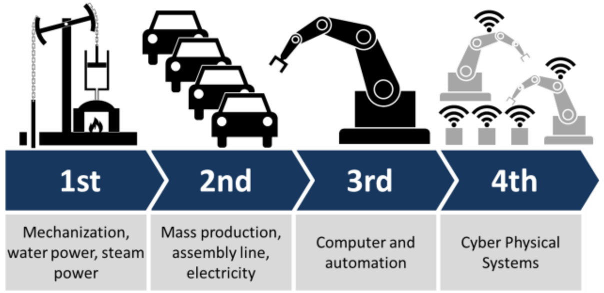
Una Organización Digital Segura es aquella que se enfoca al cliente mediante realización y adaptación de sus procesos, productos y modelos de negocio en un nuevo entorno empresarial haciendo uso de las tecnologías digitales para la mejora de su competitividad y de su relación con el cliente y otros grupos de interés (proveedores, administración, inversores, sociedad, etc.)

Fuente: Especificación UNE 0060:2018

- ✓ Procesos clave de negocio en su cadena de valor orientada al cliente;
- ✓ Productos/servicios que puedan ser transformados o complementados;
- ✓ Cambios disruptivos que más impacten en su modelo de negocio;
- ✓ Competencias y roles digitales que precisan en su actividad.

¿Qué es una “Organización Digital Segura”?





¿Qué es una "Organización Digital Segura"?

PERSEUS Cybersecurity Services

Requisitos de obligado cumplimiento o valorables

Especificación UNE
0060
Septiembre 2018

Industria 4.0
Sistema de gestión para la digitalización
Requisitos

Esta especificación ha sido elaborada por Grupo Específico de Carácter Temporal GET 24 *Procesos de transformación para la industria 4.0*, cuya secretaría desempeña UNE.

Especificación UNE
0061
Marzo 2019

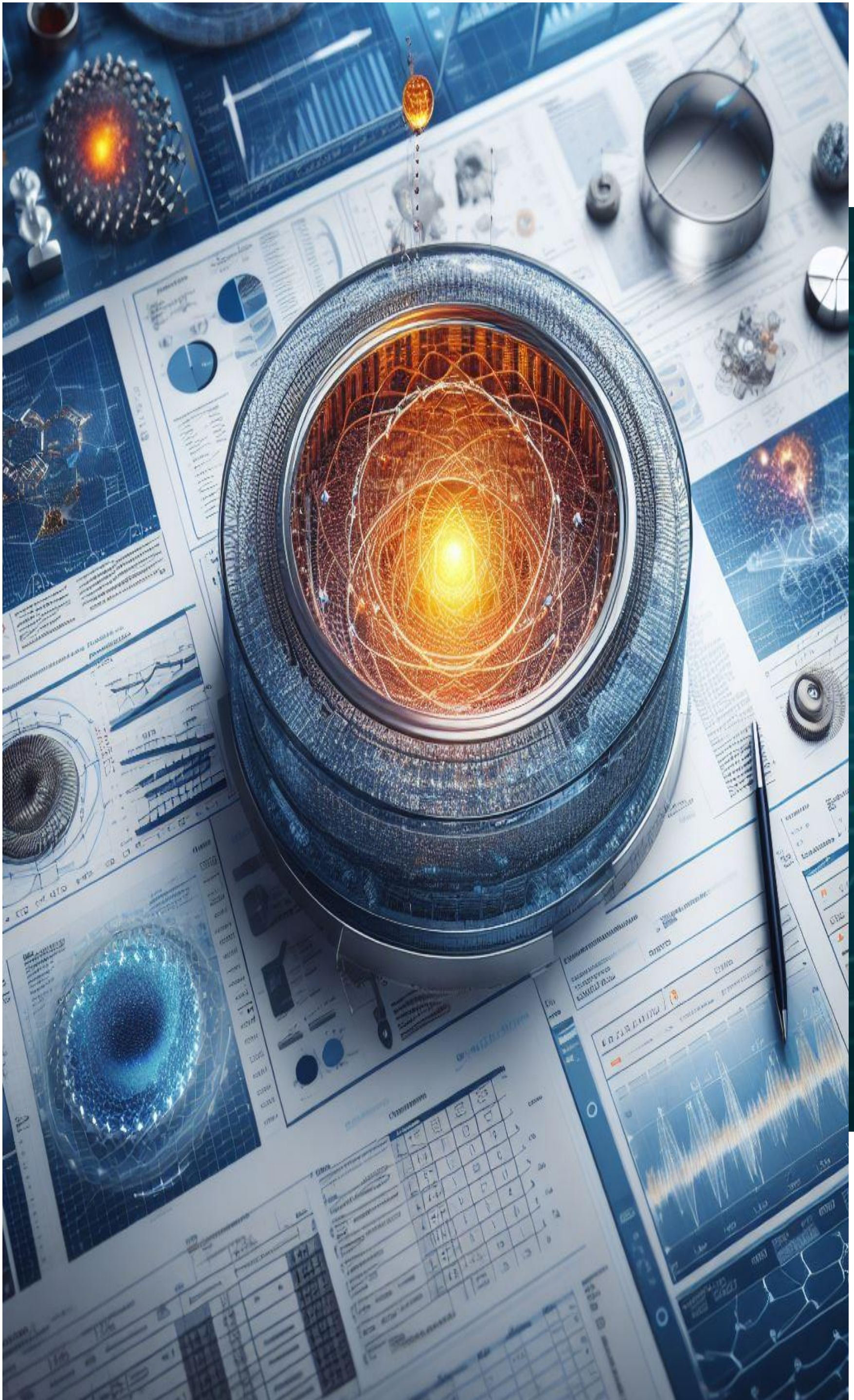
Industria 4.0
Sistema de gestión para la digitalización
Criterios para la evaluación de requisitos

Esta especificación ha sido elaborada por el Grupo Específico de Carácter Temporal GET 24 *Procesos de transformación para la industria 4.0*, cuya secretaría desempeña UNE.

Asociación Española
de Normalización
Génova, 6 - 28004 Madrid
915 294 900
info@une.org
www.une.org

Criterios de valoración

euskal IT



¿Qué es una "Organización Digital Segura"?

PERS.EUS
Cybersecurity Services

7. Operación (7.4 Visión de la Tecnología. 7.4.5 Seguridad de la Información - Ciberseguridad)

Se debe disponer de controles que aseguren la confidencialidad, integridad y disponibilidad de la información en toda la cadena de valor, incluyendo, por ejemplo, copias de backup (respaldo).

Se deben gestionar y comunicar las incidencias de seguridad detectadas de acuerdo con la normativa vigente.

Se debe asegurar la protección de los datos y los derechos de propiedad, proporcionando a todas las partes interesadas el control de sus datos y fomentando la transparencia en lo relativo a sus derechos como usuarios digitales de productos y servicios – Privacy by design.

Se debe asegurar que la organización y sus proveedores cumplen la política de seguridad de la información, mediante acuerdos y la implantación de controles oportunos que garanticen su cumplimiento.

Implantar controles de seguridad adecuados para la protección de dispositivos móviles e IoT.

Se debe asegurar que los empleados reciban formación y concienciación en materia de seguridad.

Deben existir mecanismos para clasificar la información en función del nivel de protección que necesite.

Deben existir mecanismos para controlar los accesos físicos y lógicos.

Fuente: Especificación UNE 0061

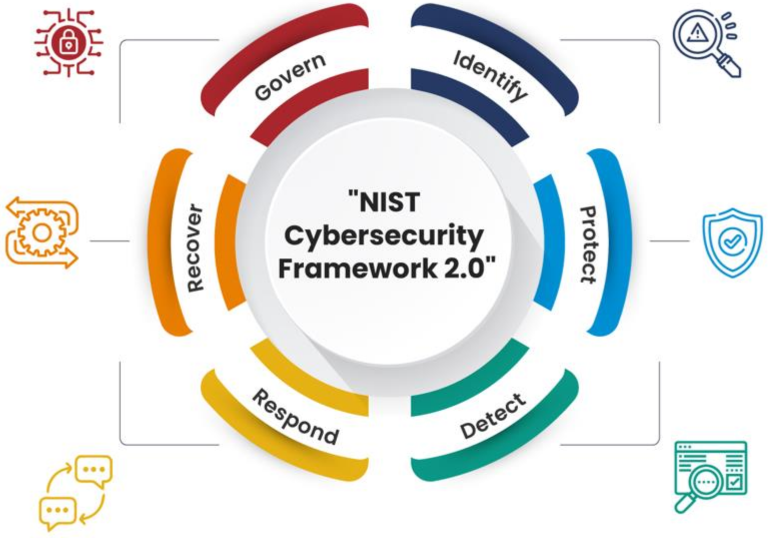
euskalIT

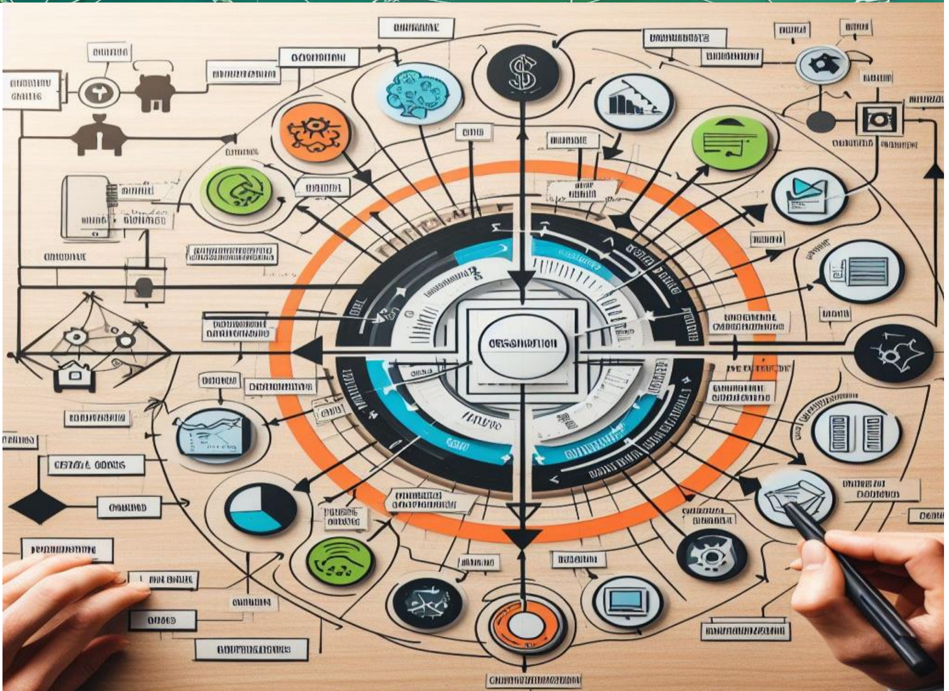
Gestionando la ciberseguridad

[NIST Cybersecurity Framework v1.1]

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover





Gestionando la ciberseguridad (Identificar)

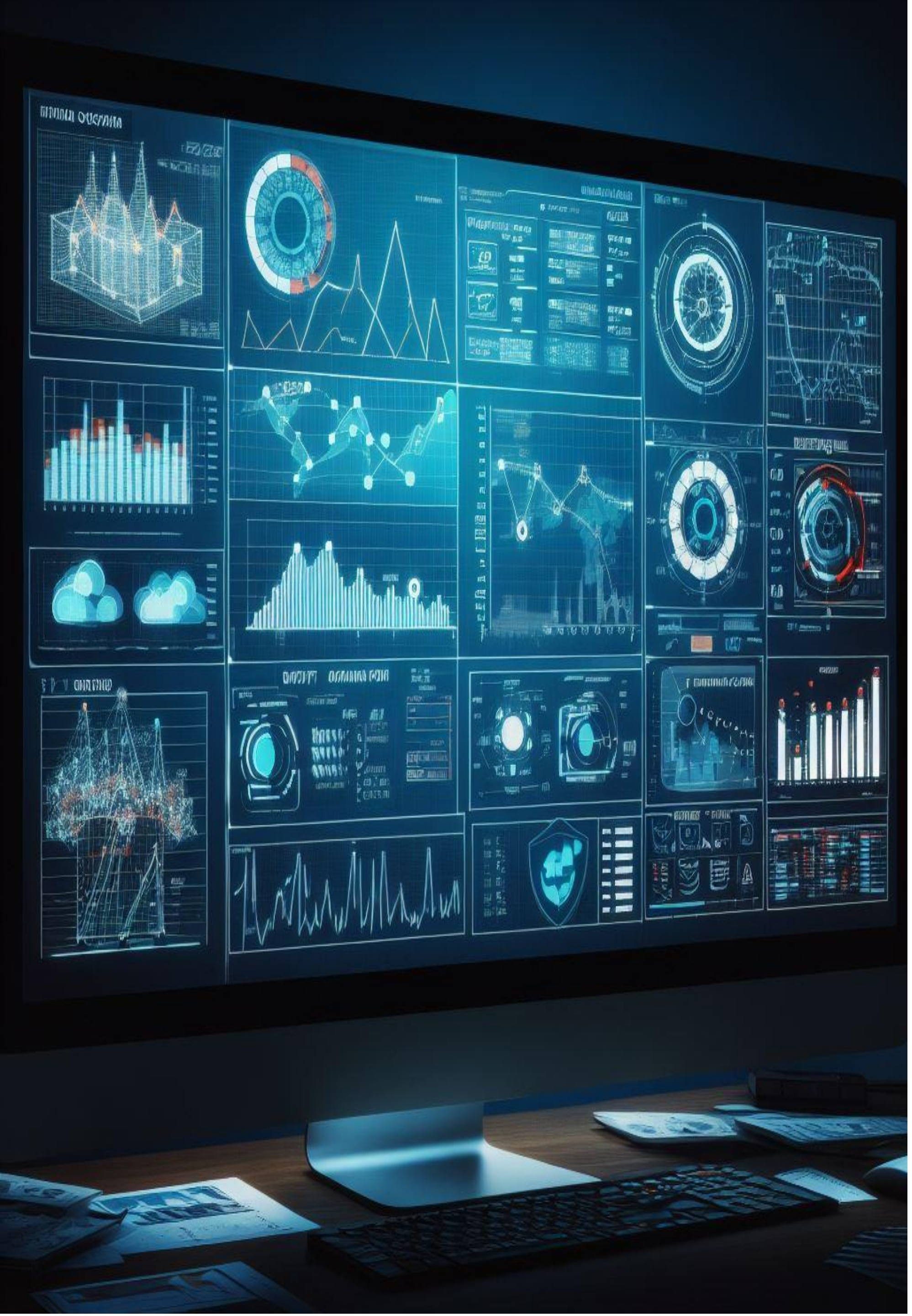
- ✓ **Entorno empresarial:** Los objetivos y requisitos de la organización se determinan y priorizan en relación con su necesidad de protección.
- ✓ **Gobernanza**: Las políticas, procedimientos y procesos de la organización para gestionar y supervisar el riesgo de ciberseguridad se establecen y actualizan.
- ✓ **Gestión de activos:** Los activos físicos y lógicos dentro del entorno de la organización se identifican, catalogan y gestionan.
- ✓ **Evaluación de riesgos:** El riesgo potencial para los activos, las operaciones, los empleados y terceros se identifica y analizan.
- ✓ **Estrategia de riesgos:** La tolerancia al riesgo de la organización se determina y se expresa, y se implementan los procesos para coordinar las decisiones sobre el riesgo.
- ✓ **Gestión de la cadena de suministro:** Los riesgos asociados a los proveedores y otros terceros se identifican y gestionan.

Gestionando la ciberseguridad (Proteger)

PERS.EUS
Cybersecurity Services

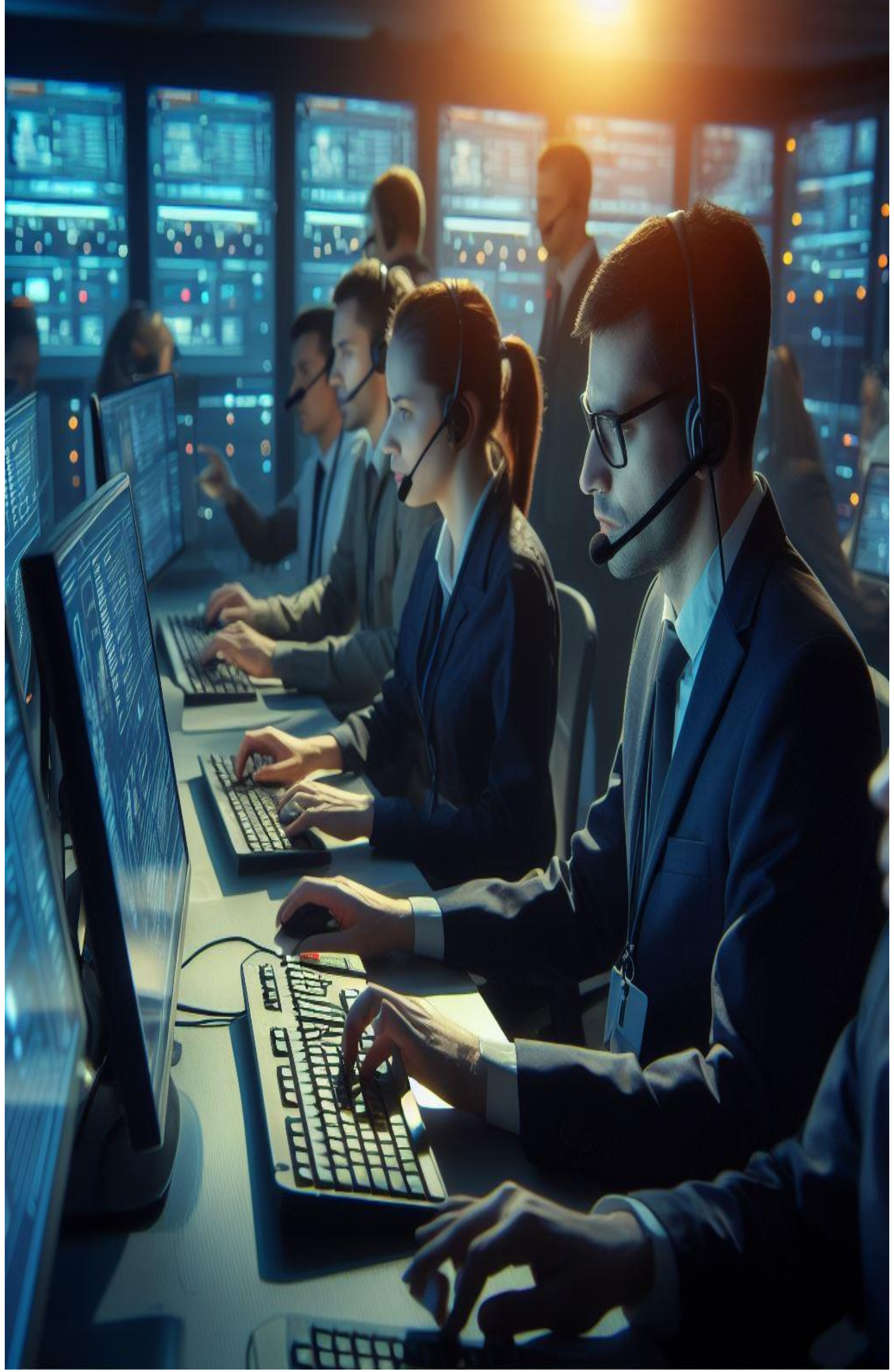
- ✓ **Control de acceso**: El acceso a los activos y servicios se limita según lo necesario para mantener la seguridad.
- ✓ **Concienciación y formación**: El personal y los proveedores están informados y capacitados sobre sus roles y responsabilidades en materia de ciberseguridad.
- ✓ **Seguridad de los datos**: Los datos se gestionan de forma segura durante todo su ciclo de vida, desde la creación hasta la eliminación.
- ✓ **Mantenimiento de la información**: Los recursos se mantienen para reducir la vulnerabilidad frente la amenaza que supone la obsolescencia.
- ✓ **Protección de infraestructuras**: Las infraestructuras físicas y lógicas se protegen frente a amenazas externas e internas.
- ✓ **Seguridad del entorno operativo**: Las operaciones se realizan con seguridad mediante la gestión del cambio, la protección frente al malware, las copias de seguridad, redundancias, etc.

euskal IT



Gestionando la ciberseguridad (Detectar)

- ✓ **Análisis de anomalías y eventos:** Se identifican situaciones anómalas y eventos potencialmente perjudiciales para determinar el impacto en la seguridad de la organización.
- ✓ **Monitorización continua de la seguridad:** Se monitorizan los activos, para detectar eventos de seguridad.
- ✓ **Detección de anomalías**: Se mantienen y prueban los procesos de detección.



Gestionando la ciberseguridad (Responder)

- ✓ **Preparación de la respuesta**: Se mantienen y prueban los procesos de respuesta.
- ✓ **Comunicaciones**: Las actividades de respuesta se coordinan con las partes interesadas internas y externas.
- ✓ **Análisis**: Se analizan las notificaciones de incidentes actuales y pasadas para garantizar una respuesta efectiva.
- ✓ **Mitigación**: Se realizan actividades para prevenir la expansión de un evento, mitigar sus efectos y resolver el incidente.
- ✓ **Mejoras**: Las actividades de respuesta se mejoran incorporando las lecciones aprendidas de las actividades actuales y anteriores.

Gestionando la ciberseguridad (Recuperar)

PERS.EUS
Cybersecurity Services

- ✓ **Recuperación gestionada**: Los procesos y procedimientos de recuperación se planifican, ejecutan, prueban y mantienen para garantizar la restauración oportuna de los sistemas o activos afectados por incidentes de ciberseguridad.

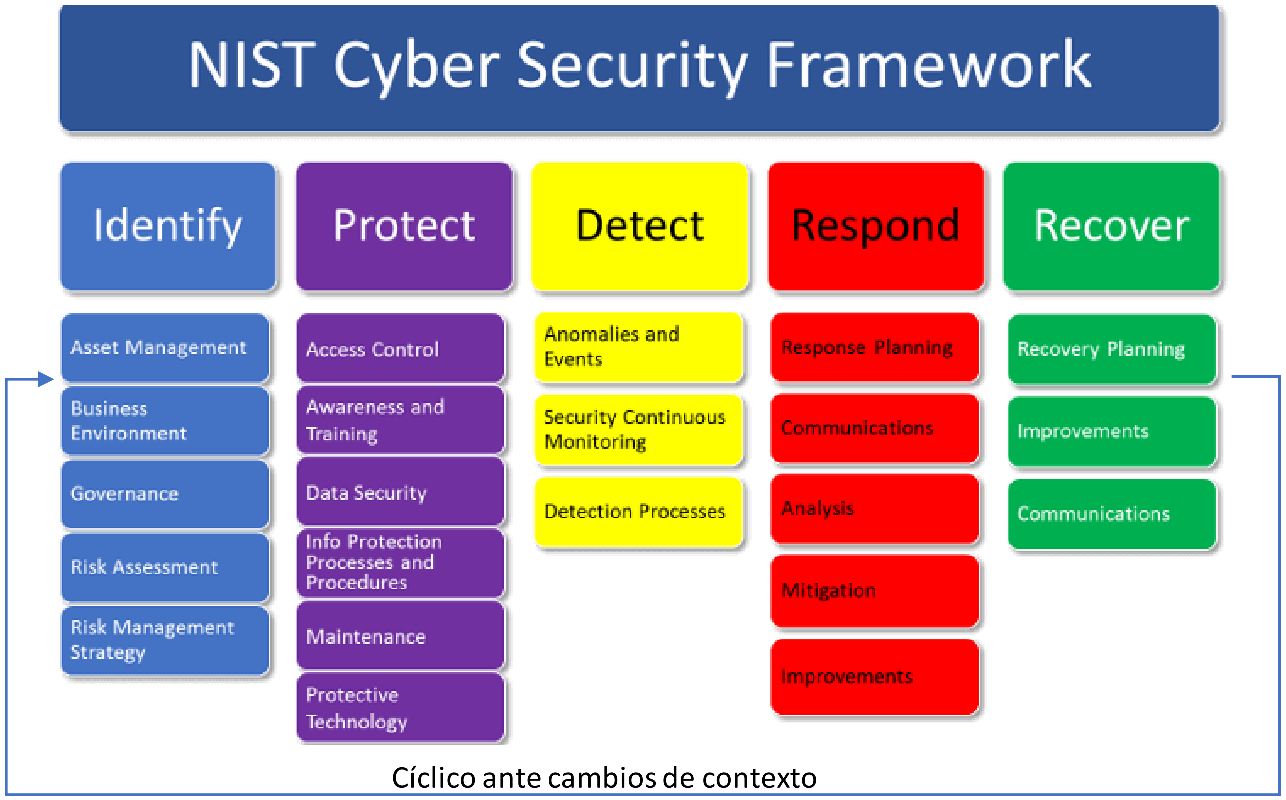
- ✓ **Mejoras**: La planificación y los procesos de recuperación se mejoran incorporando las lecciones aprendidas en futuras actividades.

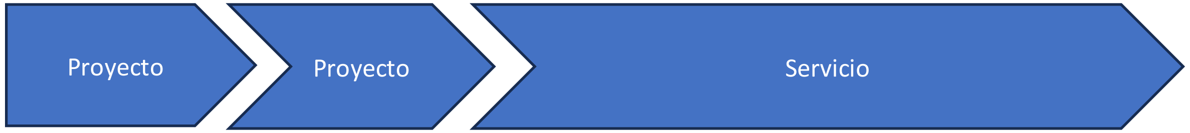
- ✓ **Comunicaciones**: Las actividades de restauración se coordinan con las partes interesadas internas y externas.

euskal IT

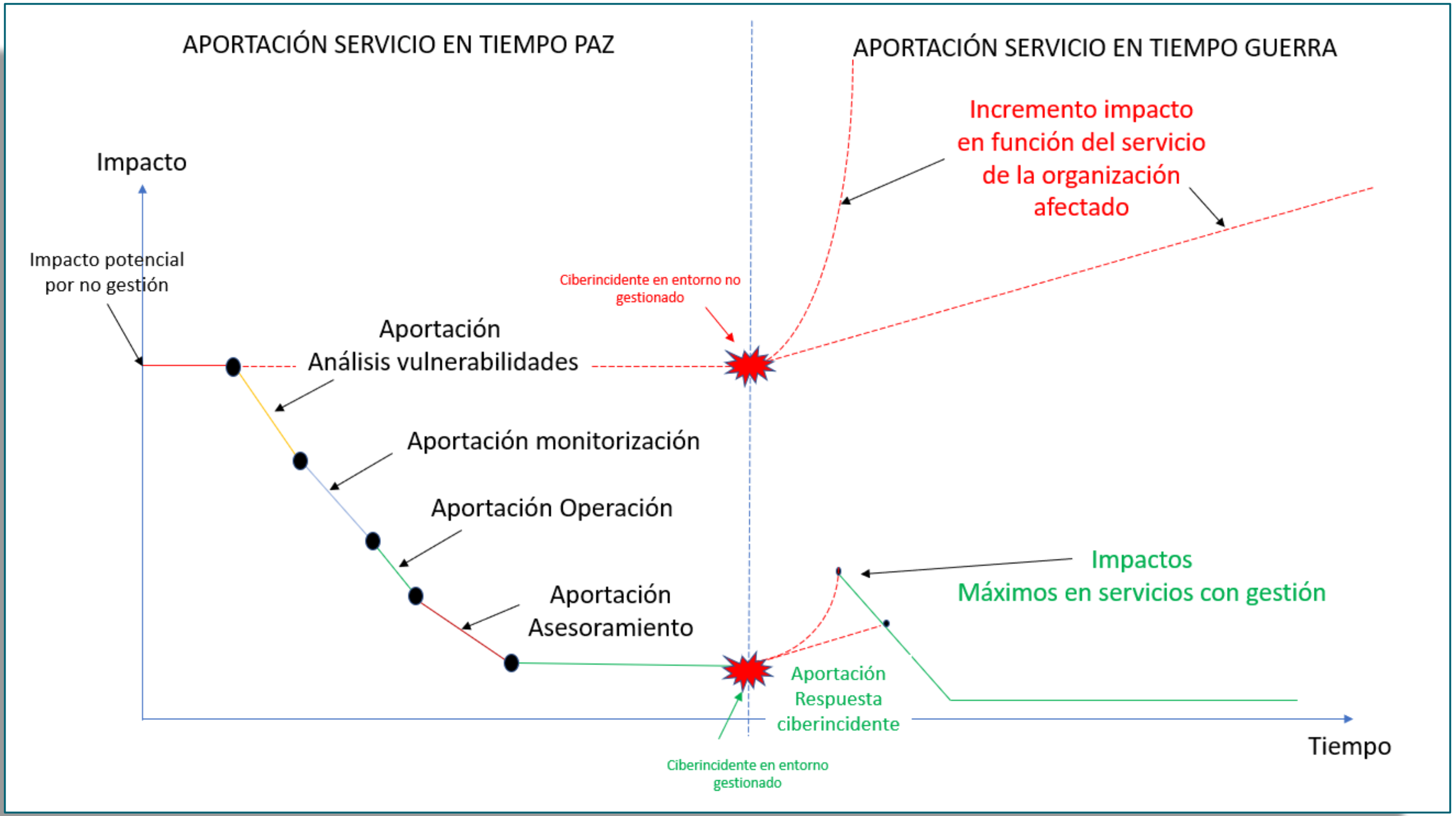
Gestionando la ciberseguridad

[NIST Cybersecurity Framework v1.1]





¿Qué es un servicio de SOC o de Ciberseguridad Gestionada?



Conclusiones

- ✓ La transformación digital es inherente a la supervivencia de las organizaciones.
- ✓ El ámbito digital “empapa” todos los procesos, productos y servicios.
- ✓ La amenaza es global, no local como ocurría en el mundo “físico”.
- ✓ Los modelos de gestión existen para aportar al negocio optimizando los recursos empleados.
- ✓ Nuestro entorno es maduro en ayudar a proteger y recuperar.
- ✓ Apóyate en especialistas para priorizar y avanzar.

Eskerrik asko!

Joserra.concha@pers.eus