VII CONGRESO SMART GRIDS
Madrid, 16 diciembre 2020

MODELO DE CONCIENCIACIÓN Y BUENAS PRÁCTICAS EN CIBERSEGURIDAD PARA EMPRESAS DEL SECTOR ELÉCTRICO

Iñaki Angulo

Gestor de Proyectos de I+D

TECNALIA

CIBERSEGURIDAD

Tecnología

Procesos

Personas

SDN-µSense

- Desarrollar un conjunto de herramientas para mejorar la resiliencia y privacidad de las redes eléctricas a los ciberataques.
- Modelo de Concienciación y Buenas Prácticas en Ciberseguridad

EPES User Role Catalogue (knowledge, skills, abilities)

Cybersecurity Capability Maturity Model

Evaluation Tool

El proyecto SDN-microSENSE ha recibido financiación del programa de investigación e innovación Horizonte 2020 de la Unión Europea en virtud del acuerdo de subvención N.º 833955. La información contenida en este artículo refleja únicamente la opinión de los autores. La Comisión Europea no se hace responsable del uso que pueda hacerse de esta información.

CATÁLOGO

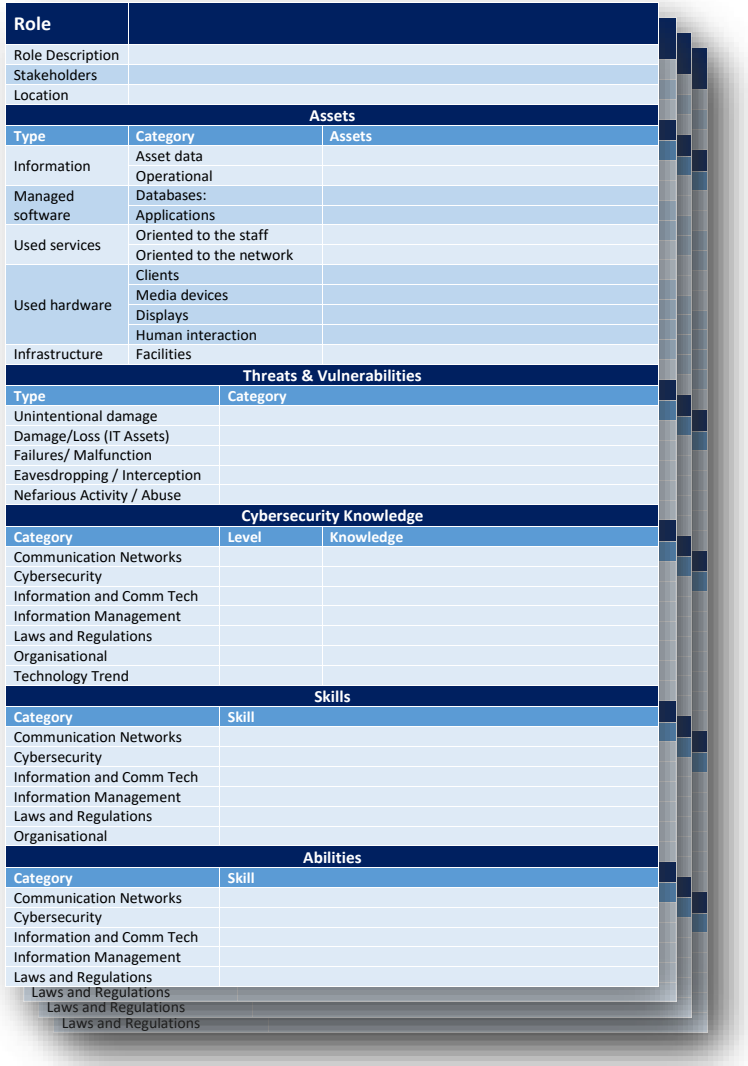
Actividad de la compañía
Puesto de trabajo

Identificación de los activos

Amenazas y vulnerabilidades

Conocimientos en Ciberseguridad

Habilidades en Ciberseguridad



Role	
Role Description	
Stakeholders	
Location	

Assets		
Type	**Category**	**Assets**
Information	Asset data	
	Operational	
Managed software	Databases:	
	Applications	
Used services	Oriented to the staff	
	Oriented to the network	
Used hardware	Clients	
	Media devices	
	Displays	
	Human interaction	
Infrastructure	Facilities	

Threats & Vulnerabilities	
Type	**Category**
Unintentional damage	
Damage/Loss (IT Assets)	
Failures/ Malfunction	
Eavesdropping / Interception	
Nefarious Activity / Abuse	

Cybersecurity Knowledge		
Category	**Level**	**Knowledge**
Communication Networks		
Cybersecurity		
Information and Comm Tech		
Information Management		
Laws and Regulations		
Organisational		
Technology Trend		

Skills	
Category	**Skill**
Communication Networks	
Cybersecurity	
Information and Comm Tech	
Information Management	
Laws and Regulations	
Organisational	

Abilities	
Category	**Skill**
Communication Networks	
Cybersecurity	
Information and Comm Tech	
Information Management	
Laws and Regulations	

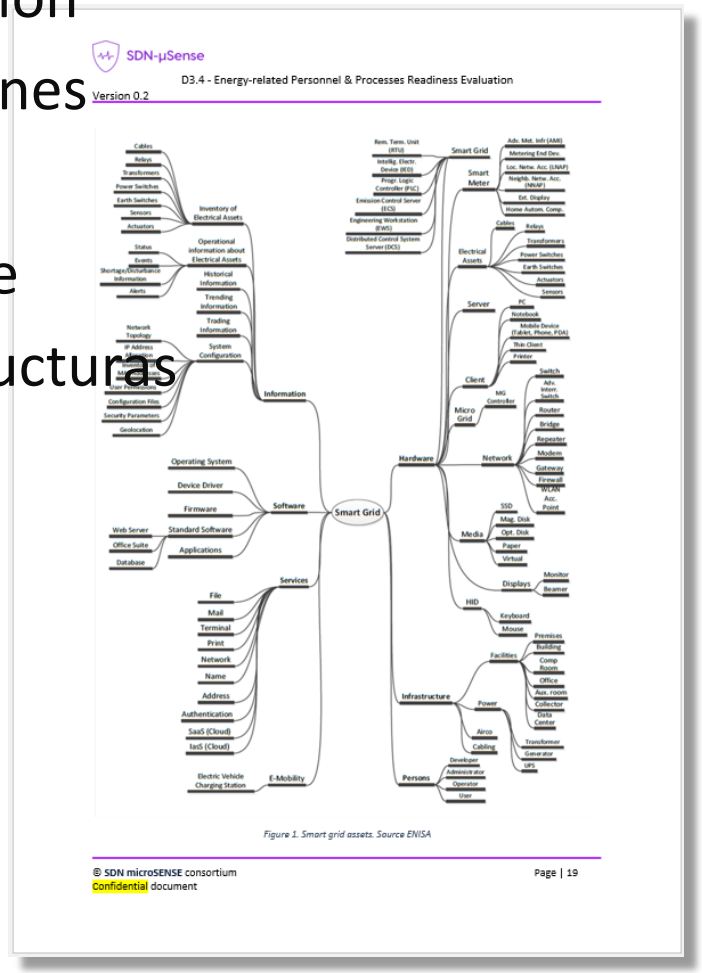
Laws and Regulations
Laws and Regulations
Laws and Regulations

1. Executive Manager
2. Security Administrator
3. Power Plant Operators
4. System Operator/Engineer
5. OT Manager/Com. Administrator
6. Substation Engineer
7. Substation Operator
8. Installer
9. Facility Operator in a Power Plant
10. Field Engineer
11. Energy Trader
12. AMI and Demand Side Manager
13. Prosumer
14. Building Energy Manager
15. Developers
16. IT User

ACTIVOS Y AMENAZAS

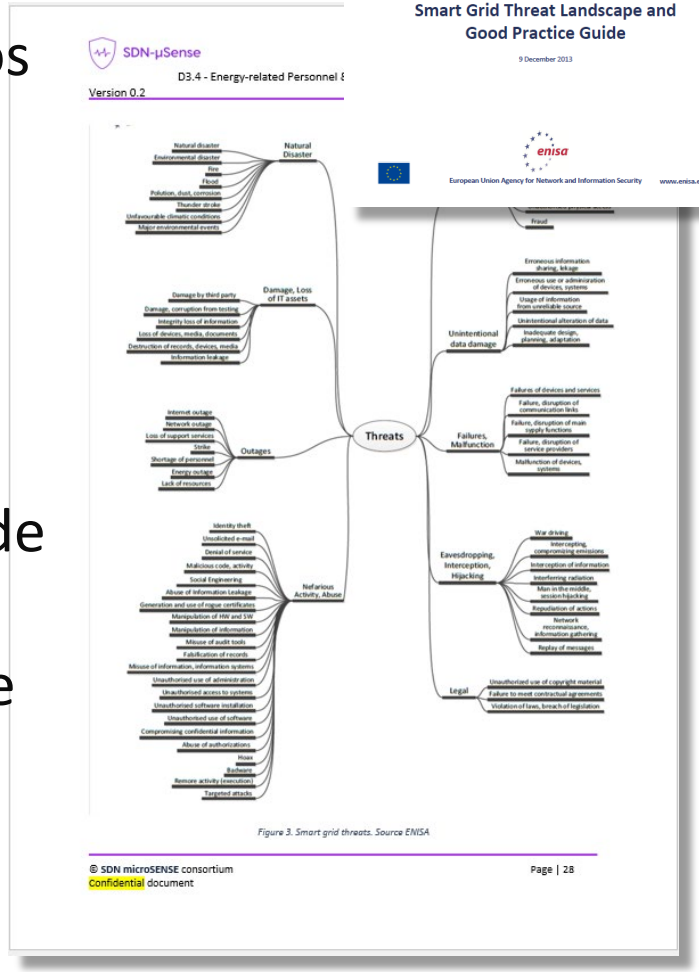
Activos:

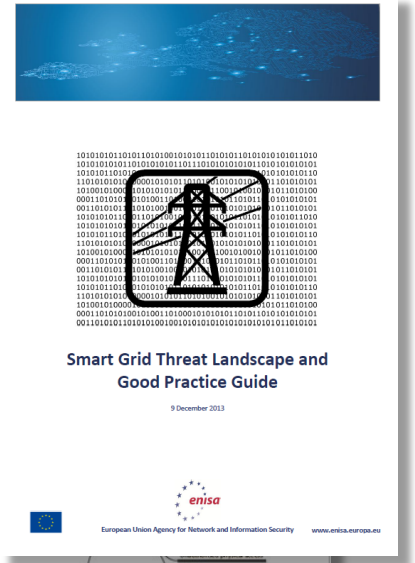
- Información
- Aplicaciones
- Servicios
- Hardware
- Infraestructuras
- Personas



Amenazas:

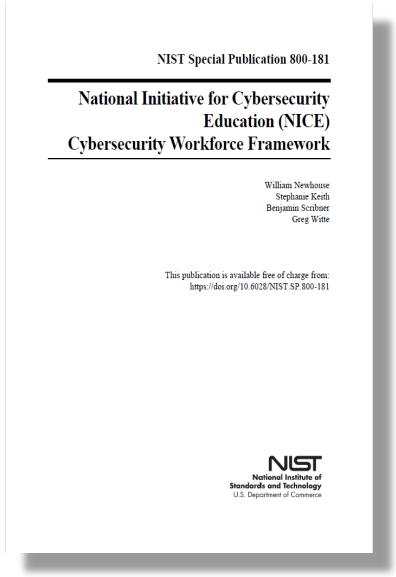
- Ataques físicos
- Daños en datos
- Desastres naturales
- Cortes de suministro
- Espionaje
- Suplantación de identidad
- Denegación de servicio
- Malware

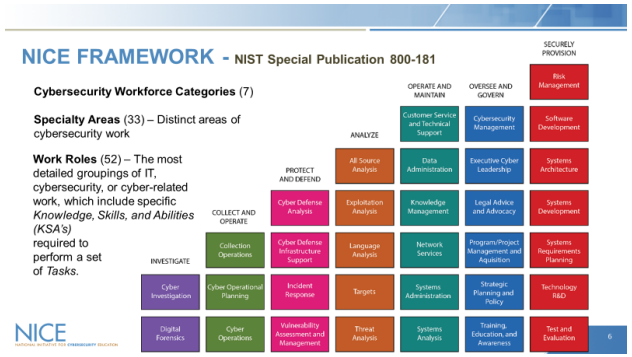


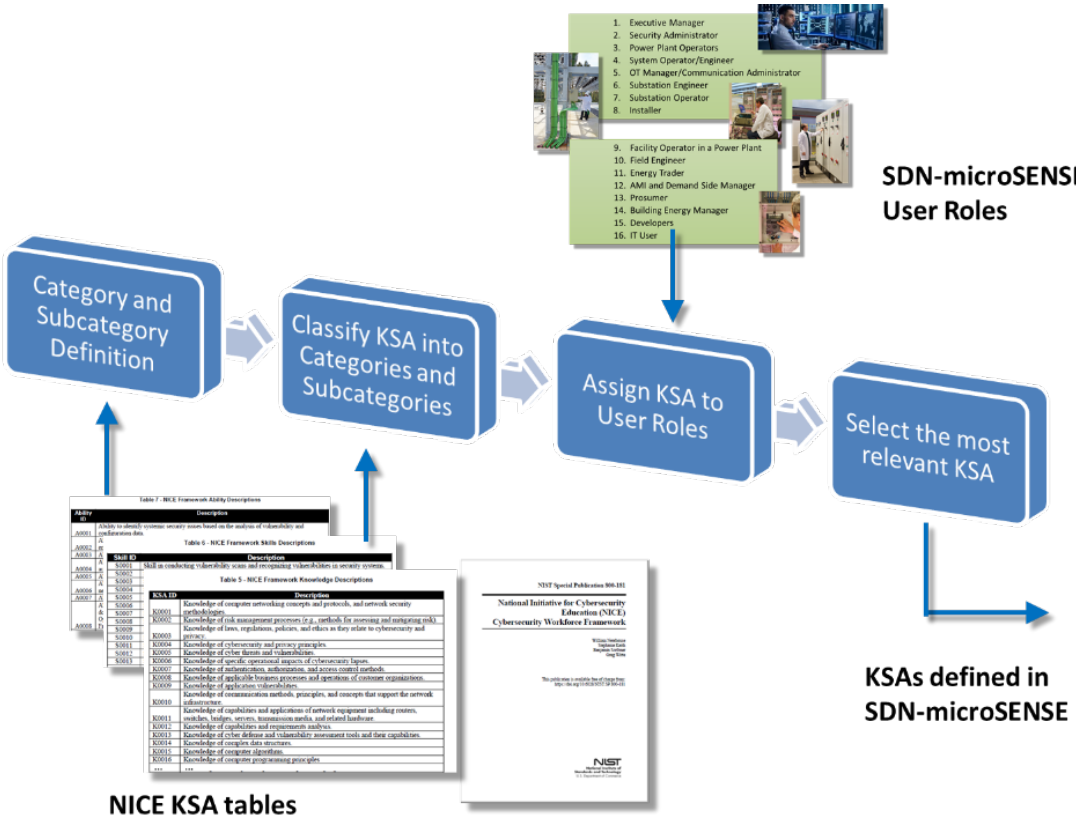


MODELO DE COMPETENCIAS EN CIBERSEGURIDAD

- National Initiative for Cybersecurity Education (NICE).
- Define el conjunto de conocimientos y habilidades en ciberseguridad específicas de una empresa eléctrica.







CONOCIMIENTOS Y HABILIDADES

Software / Hardware

Ciberseguridad

Políticas y Procesos

Redes y Comunicaciones

Gestión de la información

Tendencias Tecnológicas

Recopilación de información

Leyes y Regulación

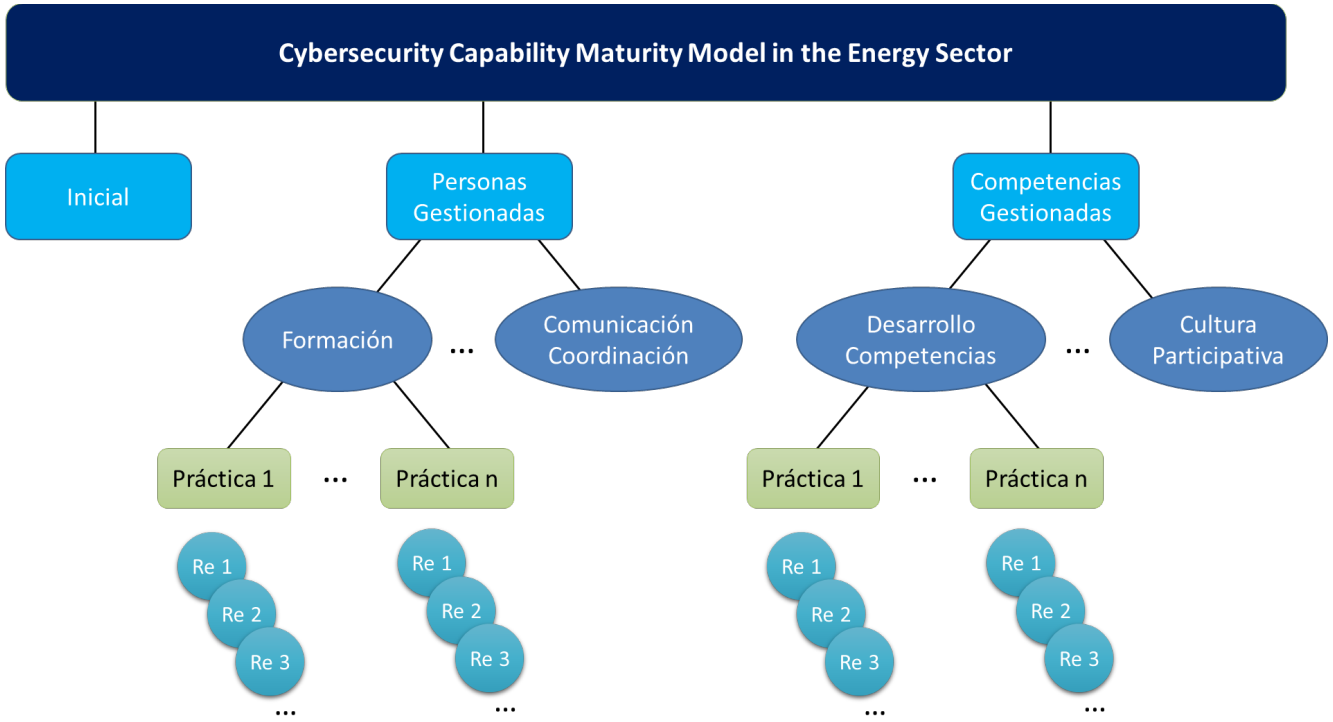
MODELO DE MADUREZ

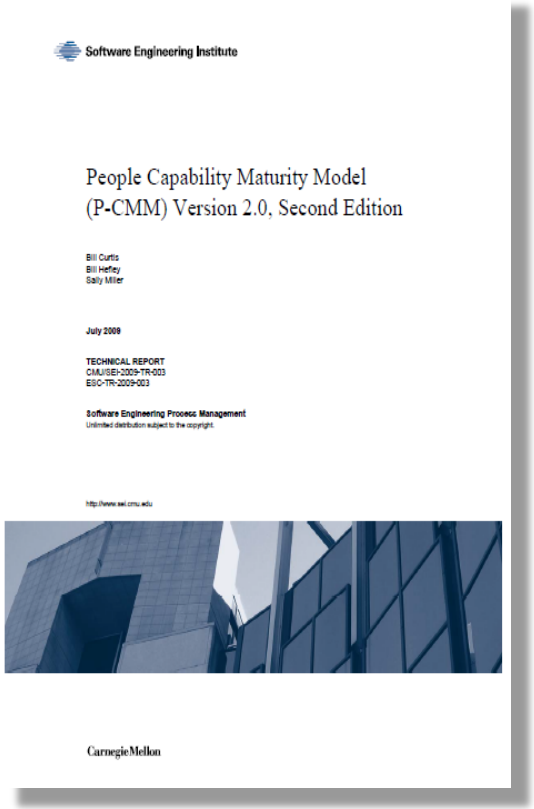
- Un conjunto de procesos y prácticas que se deben implementar en una empresa para mejorar el nivel de competencia de su personal en ciberseguridad.

3 Niveles

8 Procesos

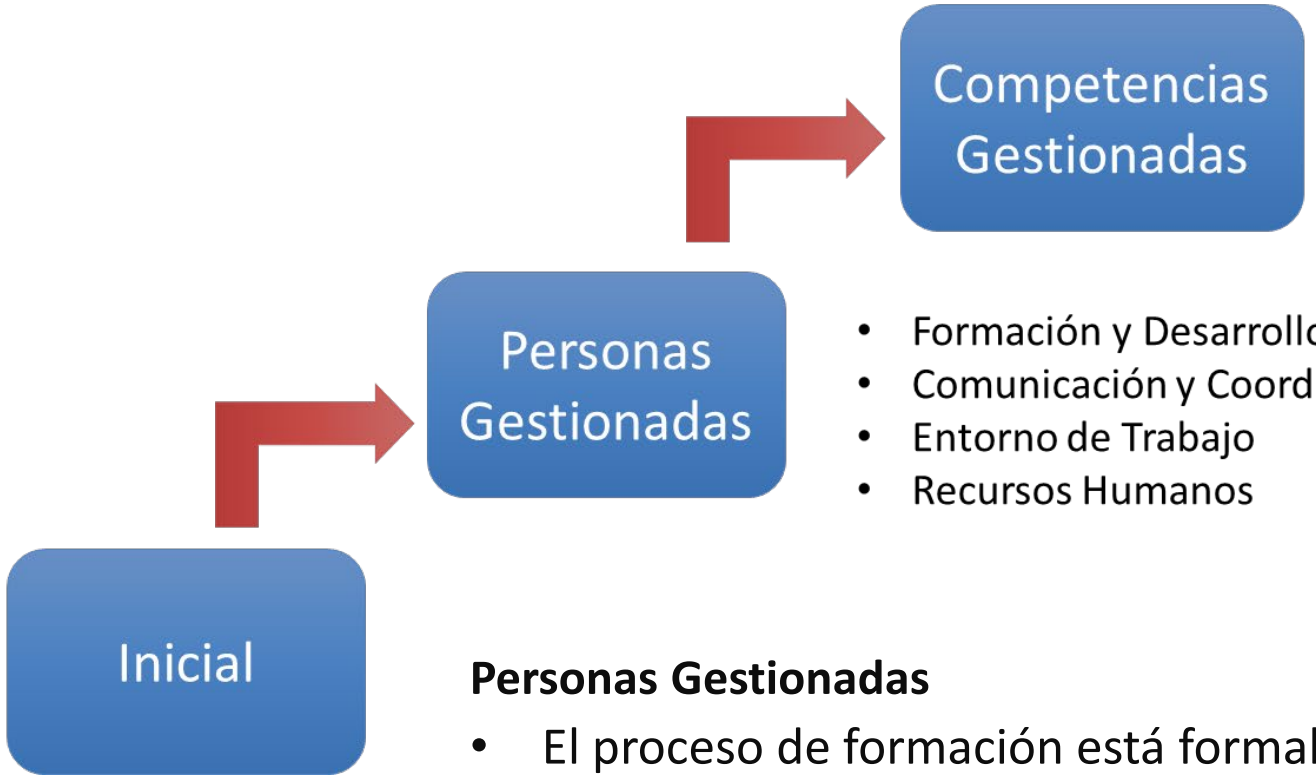
80 Prácticas





NIVELES Y PROCESOS DE MADUREZ

Modelo de Concienciación y Buenas Prácticas en Ciberseguridad para el Sector Eléctrico



- Análisis de Competencias
- Desarrollo de Competencias
- Cultura Participativa
- Planificación de Equipos de Trabajo

- Formación y Desarrollo
- Comunicación y Coordinación
- Entorno de Trabajo
- Recursos Humanos

Competencias Gestionadas

- El proceso de formación es individualizado.
- Hay una cultura participativa.
- Se adoptan prácticas y medidas en base a un proceso de evaluación de riesgos.

Personas Gestionadas

- El proceso de formación está formalizado, pero no individualizado.
- Se promueve la concienciación en ciberseguridad
- Se establecen mecanismos para informar y compartir riesgos e incidentes.

PERSONAS GESTIONADAS

Dotación de personal.

- Establecer compromisos de ciberseguridad en cada puesto de trabajo.

Formación y desarrollo.

- Asegurar la adquisición de conocimientos y habilidades en Ciberseguridad.

Comunicación y coordinación.

- Establecer mecanismos de transmisión y compartición de información.

Entorno de trabajo.

- Proporcionar un entorno de trabajo que fomente la ciberseguridad.

COMPETENCIAS GESTIONADAS

Análisis de competencias.

- Identificar los conocimientos y habilidades en ciberseguridad para cada puesto de trabajo.

Desarrollo de competencias

- Proporcionar oportunidades al personal para mejorar sus conocimientos y habilidades en ciberseguridad.

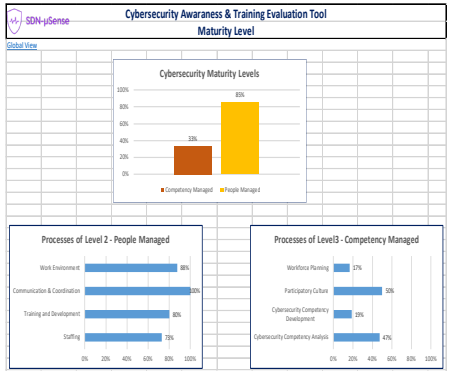
Cultura participativa

- Habilitar a los recursos humanos en la toma de decisiones.

Planificación de los recursos humanos

- Coordinar las actividades de los recursos humanos con las necesidades presentes y futuras de ciberseguridad.

PROCESO DE EVALUACIÓN



Permite medir el nivel de madurez alcanzado en una empresa en el despliegue de los procesos de formación definidos en el modelo de madurez de ciberseguridad.

Colour	The purpose of the practice is judged as
Red	Absent or poorly addressed. Deficiencies or problems were identified that will impede the achievement of the goal.
Yellow	Partially addressed. Deficiencies or problems that could threaten the achievement of the goal were identified
Green	Adequately addressed.
White	The practices are not applicable in the context of the organization.

Global View — **LEVEL 2 - PEOPLE MANAGED**

Level 2

		Satisfied	% Yes	% Partially	% Not
Staffing	Objective 1	88%	75%	25%	0%
	Objective 2	50%	50%	0%	50%
	Objective 3	67%	67%	0%	33%
	Objective 4	88%	75%	25%	0%
Training and Development	Objective 1	80%	70%	20%	10%
Communication & Coordination	Objective 1	100%	100%	0%	0%
	Objective 2	100%	100%	0%	0%
	Objective 3	100%	100%	0%	0%
Work Environment	Objective 1	100%	100%	0%	0%
	Objective 2	75%	50%	50%	0%

SDN-µSense

Cybersecurity Awaraness & Training Evaluation Tool
Level 2 - People Managed

Global View

Staffing Process

Purpose	Establish a formal process by which committed work regarding cybersecurity needs is matched to unit resources and qualified individuals are recruited, selected, and transitioned into assignments.
Objectives	
Objective 1	Individuals or workgroups in each unit are involved in making commitments that balance the unit's workload with approved staffing.
Objective 2	Candidates are recruited for open positions.
Objective 3	Staffing decisions and work assignments are based on an assessment of work qualifications and other valid criteria.
Objective 4	Individuals are transitioned into and out of positions in an orderly way.

Practices		Satisfy?	Tips
Practice 1	Each unit analyses its work to determine the cybersecurity skills required	Yes	☐ A unit's work is analyzed to determine the types of tasks that requires cybersecurity measurements and effort required to perform them. ☐ The types of skills (cybersecurity skills) needed to perform proposed work are identified
Practice 2	Individuals and workgroups participate in making commitments for cybersecurity measurements they have to adopt and perform	N/A	☐ Individuals are involved in reviewing the cybersecurity measurements to be adopted in their work ☐ Individuals or workgroups are involved in estimating the resources, effort, and schedule required to deploy cybersecurity measurements to accomplish the work that they have been allocated. ☐ Individuals or workgroups establish commitments they will be held accountable for meeting. ☐ Individuals or workgroups are involved in reviewing progress against commitments and, when necessary, making changes to the commitments regarding their work
Practice 3	Each unit documents cybersecurity commitments that balance its workload with available staff and other required resources	No	
Practice 4	Individual cybersecurity assignments are managed to balance committed cybersecurity measurements among individuals and units or groups.	N/A	

VII CONGRESO
SMART GRIDS
Madrid, 16 diciembre 2020

Iñaki Angulo

inaki.angulo@tecnalia.com

www.tecnalia.com

tecnalia Inspiring Business

SDN-µSense

https://www.sdnmicrosense.eu/