Cybersecurity skills framework

Approach

Global defines the baseline of the Group

Local adaptation enriched with more detail if required

Businesses specifics training paths for profiles/skills that are unique to them

Profiles

Board of Directors

BISOS

Executive Leadership

General Employees

Executive Assistants

Technical Employees

CISOS

Field Employees

Levels

Level 4 - Expert/Proactive

People with high experience in the role and strong involvement in the cybersecurity culture.

Objective: To integrate cybersecurity into the culture and strategy of the area.

Level 3 - Advanced/Reactive

People with experience in the role and previous training in cybersecurity.

Objective: To train to act in the event of incidents and support the response.

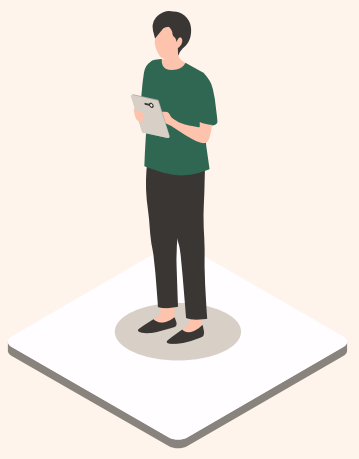
Level 2 - Intermediate/Conscious

People with some experience in the role and exposure to basic cybersecurity training.

Objective: To consolidate good practices and contextualise risks.

Level 1 - Basic/Initiated

People new to the role or without previous training in cybersecurity.



Objective: To raise awareness and teach basic practices.

Catalogs

There are different content catalogues created for the various roles within the company. Within them, we have established the main cyber competency frameworks across Iberdrola's structure, in accordance with the level of knowledge and responsibility associated with each itinerary.

Expert/Proactive *Advanced/Reactive* *Intermediate/Conscious* *Basic/Initiated*