

# Marco de competencias en ciberseguridad

## Enfoque



El nivel global define la base de referencia del Grupo

Adaptación local enriquecida con más detalles si es necesario

Itinerarios formativos específicos para cada negocio, adaptados a los perfiles y competencias propios de cada uno

## Perfiles

Consejo de Administración



Dirección ejecutiva



Asistentes ejecutivos



CISOS



BISOS



Empleados generales



Empleados técnicos



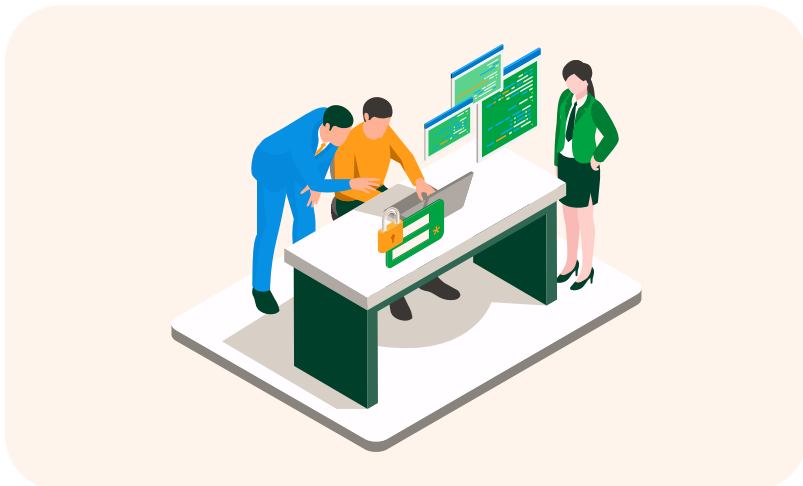
Empleados de campo



## Niveles

### Nivel 4 - Experto/Proactivo

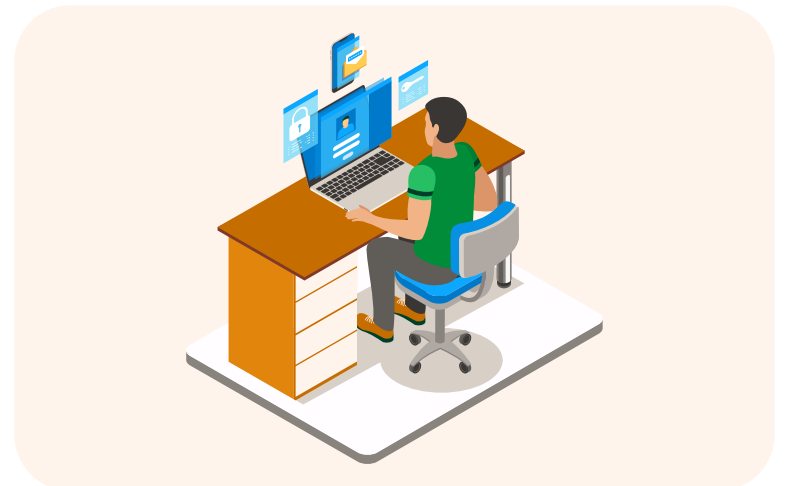
Personas con gran experiencia en el puesto y una fuerte implicación en la cultura de la ciberseguridad.



**Objetivo:** Integrar la ciberseguridad en la cultura y la estrategia del área.

### Nivel 3 - Avanzado/Reactivo

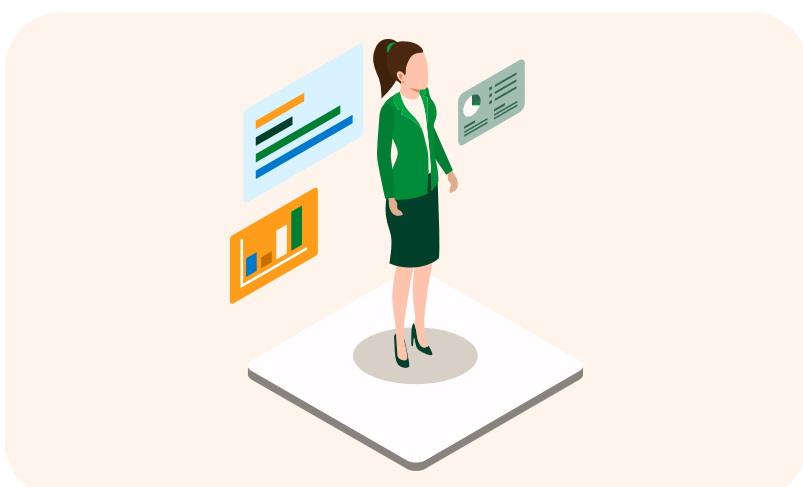
Personas con experiencia en el puesto y formación previa en ciberseguridad.



**Objetivo:** Formar para actuar en caso de incidentes y apoyar la respuesta.

### Nivel 2 - Intermedio/Consciente

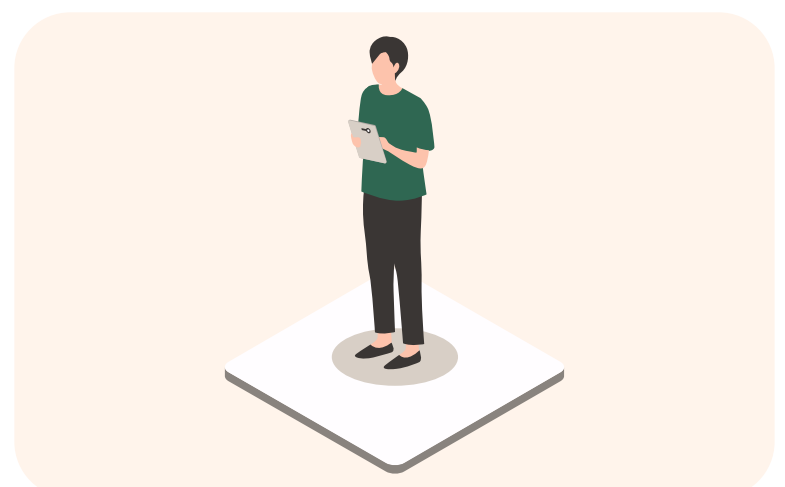
Personas con cierta experiencia en el puesto y que han recibido formación básica en ciberseguridad.



**Objetivo:** Consolidar buenas prácticas y contextualizar los riesgos.

### Nivel 1 - Básico/Iniciado

Personas nuevas en el puesto o sin formación previa en ciberseguridad.



**Objetivo:** Sensibilizar y enseñar prácticas básicas.

## Catálogos

Existen diferentes catálogos de contenido creados para los diferentes roles dentro de la compañía. Y en ellos, hemos establecido los principales marcos de competencias cibernéticas dentro de la estructura de Iberdrola, de conformidad con el nivel de conocimiento y responsabilidad de cada itinerario.

Experto/Proactivo Avanzado/Reactivo Intermedio/Consciente Básico/Iniciado