CIBERSEGURIDAD ETHICAL HACKING PENETRATION TESTING FORMACIÓN

ISGroup
Information Security

Compliance NIS2

Gap analysis, plan de remediación y formación para lograr y mantener la conformidad

OBJETIVO

Convierte obligaciones y plazos en un programa de resiliencia

La Directiva NIS2 exige gobernanza, gestión de riesgos, medidas técnicas y capacidad de respuesta demostrables.

ISGroup traduce los requisitos en prioridades operativas coherentes con organización, sector y exposición.

ISGroup
Information Security

MÉTODO

Del gap analysis a un plan ejecutable y verificable

Evaluación

Mapeamos alcance, obligaciones, gobernanza y medidas existentes.

Plan

Ordenamos las acciones por riesgo, dependencias, costes y plazos.

Implantación

Apoyamos controles, procedimientos, formación y recopilación de evidencias.

ISGroup
Information Security

MODALIDAD

Gobernanza, supply chain, incidentes y continuidad operativa

El recorrido cubre gestión de riesgos, proveedores, vulnerabilidades, accesos, backup y respuesta a incidentes.

Los roles del management se formalizan mediante flujos de escalado y reporting.

La formación y los ejercicios hacen efectivas las medidas en las operaciones diarias.

ISGroup
Information Security

PUNTOS FUERTES

Competencias GRC y técnicas en el mismo equipo

Cobertura

Requisitos organizativos, documentales y tecnológicos evaluados juntos.

Prioridades

Acciones ordenadas según riesgo real y capacidad de ejecución.

Evidencias

Decisiones, controles y verificaciones documentados para auditorías.

ISGroup
Information Security

OUTPUT

Una roadmap NIS2 con responsables, plazos y evidencias

Gap analysis frente a los requisitos aplicables.

Plan de remediación priorizado con responsables y plazos.

Registro de evidencias para medidas, formación y verificaciones.

Reporting directivo sobre avance y riesgo residual.

ISGroup
Information Security

Let's HACK together

ISGroup
Information Security

CF e P.IVA 04164220230
www.isgroup.it

RESERVA UNA CITA
sales@isgroup.it
+39 045 4853232