Escuela de organización industrial

Cabildo de Gran Canaria

spegc
Sociedad de Promoción Económica

PROGRAMA EJECUTIVO EN

Ciberseguridad

GRAN CANARIA - SEMIPRESENCIAL

La ciberseguridad es el campo de estudio y aplicación de técnicas, procesos y recursos necesarios para luchar contra los riesgos que menazan, desde múltiples ángulos, a las empresas y su capacidad de ejecutar su misión (venta de bienes, provisión de servicios...).

Introducción

La ciberseguridad es el campo de estudio y aplicación de técnicas, procesos y recursos necesarios para luchar contra los riesgos que amenazan, desde múltiples ángulos, a las empresas y su capacidad de ejecutar su misión (venta de bienes, provisión de servicios...).
La transformación digital en la que está inmerso ahora mismo el tejido empresarial mundial implica diversos cambios culturales, adopción tecnológica, nuevos procesos, etc., pero en todo ello es fundamental que el entorno digital sea estable y seguro.

La ciberseguridad requiere, como cualquier otra disciplina fundamental, de toda una vida para dominar a nivel experto cualquiera de sus ámbitos y su aplicación a los procesos digitales; pero de cara a cualquier profesional que aborde la ciberseguridad en cualquiera de sus ámbitos, es necesario disponer de un nivel de conocimiento de lo fundamental, que le permita distinguir lo importante de lo accesorio y entender la relevancia de un incidente, una noticia, una normativa aplicable o qué solución nos propone el departamento técnico o un proveedor.

En esta formación se recorrerán a nivel de introducción los principales componentes que explican esa relevancia de la ciberseguridad y que solo va a crecer en los próximos años conforme se incremente la adopción de nuevas tecnologías, los riesgos asociados, los incidentes de seguridad y las regulaciones que buscarán resolverlos.

El objetivo de la formación es dotar a los alumnos de las herramientas necesarias para, no sólo defenderse sino también poder liderar iniciativas de seguridad en sus carreras profesionales, reforzando conocimientos especializados en ciberseguridad on el repaso amplio de esta competencia y sobre todo su contextualización en el ámbito de la empresa

INICIO
Mayo

DURACIÓN
218 horas:
• 40 presenciales
• 128 online
• 50 proyecto

HORARIO CLASES PRESENCIALES
Viernes tarde
Sábados mañana

MODALIDAD
Semipresencial

LUGAR SESIONES PRESENCIALES
Gran Canaria

PRECIO
Precio: 4.400 €
Precio Bonificado: 440 € en concepto de matrícula

25 Plazas bonificadas gracias a la aportación económica de la Sociedad de Promoción Económica de Gran Canaria (SPEGC)

Dirigido a

- Directivos, gerentes y trabajadores que deseen entender la tecnología que usan en su día a día, conocer los riesgos que implica su uso y aprender cómo proteger la empresa o área de negocio.

- Perfiles que quieran incorporarse a al ámbito de ciberseguridad y quieran tener un primer contacto con ella.

- La capacidad y experiencia del equipo docente permite, en caso de ser necesario, profundizar más en las cuestiones que donde los alumnos lo requieran.

La selección de los/as participantes se realizará entre las solicitudes recibidas en función de los criterios de valoración publicados en la convocatoria, teniendo preferencia los profesionales de empresas e instituciones públicas con domicilio social en Gran Canaria.

Consulta las bases de esta convocatoria en
www.eoi.es/programas/becas-y-descuentos

Contenidos

INTRODUCCIÓN A LA CIBERSEGURIDAD. CONCEPTOS BÁSICOS

- Ciberseguridad, amenazas, vulnerabilidades y riesgos.
- Componentes básicos de la seguridad, actores en la ciberdelincuencia.
- Procesos básicos de ciberseguridad.

GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN

- Modelos, controles, nivel de madurez.
- Regulación y normativa.

GESTIÓN DE RIESGOS

- Definición, metodologías, análisis.
- Tratamiento y monitorización.

PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN

- Qué proteger.
- Qué tecnologías.
- Qué procedimientos.
- Definición de estrategia.

CIBERINTELIGENCIA

- Definición, tipos, OSINT.
- Aplicación a escenarios reales.

HACKING ÉTICO

- Fases de un ataque.
- Reconocimiento.
- Ataques sobre infraestructura.
- Aplicaciones web.
- Ingeniería social.

GESTIÓN DE INCIDENTES

- Definición, metodologías, fases.
- Ámbito técnico y de gestión.
- Comunicación y comité de crisis.

PLAN DE CONTINUIDAD DE NEGOCIO

- Planes de continuidad de negocio.
- Planes de contingencia.
- Recuperación de desastres.
- Tiempos de recuperación (RTO, RPO), BIA (Business Impact Analysis).

LA NUBE

- Definición.
- Tipos.
- Modelos de responsabilidad.
- Ventajas e inconvenientes.
- Servicios.

CIBERSEGURIDAD EN EL ÁMBITO INDUSTRIAL

- Definición.
- IT vs OT.
- Cómo aplicar seguridad.
- Problemas y soluciones.
- Servicios.

PROTECCIÓN DE DATOS

- Tipos de datos.
- Clasificación de la información.
- Tecnologías.
- Cómo realizar una aproximación inicial.

CONCIENCIACIÓN

- El empleado como primera línea de defensa.
- Principales vectores de ataque y riesgos en función de los roles.
- Cómo diseñar un programa integral de concienciación.
- Qué métricas son importantes para evaluar estado y evolución.

PROYECTO

Como parte de la formación se realizará un proyecto académico, desde su concepción hasta su diseño e implementación, que permitirá poner en práctica todos los conocimientos adquiridos.

Formamos
talento para un futuro sostenible

Madrid
informacion@eoi.es
+34 91 349 56 00
(Madrid)

Sevilla
infoandalucia@eoi.es
+34 95 446 33 77
(Sevilla)

Elche
eoimediterraneo@eoi.es
+34 96 665 81 55
(Elche – Alicante)

www.eoi.es

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO · EOI Escuela de organización industrial

Cabildo de Gran Canaria · spegc Sociedad de Promoción Económica