Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

RESPONSABLE DE CIBERSEGURIDAD EN EL ÁMBITO EMPRESARIAL

Septiembre 2024

GOBIERNO DE ESPAÑA
MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL
SERVICIO PÚBLICO DE EMPLEO ESTATAL
SEPE

SISTEMA NACIONAL DE EMPLEO

IDENTIFICACIÓN DE LA ESPECIALIDAD Y PARÁMETROS DEL CONTEXTO FORMATIVO

Denominación de la especialidad:	RESPONSABLE DE CIBERSEGURIDAD EN EL ÁMBITO EMPRESARIAL
Familia Profesional:	ADMINISTRACIÓN Y GESTIÓN
Área Profesional:	ADMINISTRACIÓN Y AUDITORÍA
Código:	ADGD0074
Nivel de cualificación profesional:	3

Objetivo general

Desempeñar el rol de responsable de ciberseguridad dirigiendo y gestionando la política de seguridad de la información de la organización, definiendo la estrategia y su implementación, estando a cargo del diseño, prevención, asesoramiento, supervisión, identificación, detección, respuesta, recuperación, coordinación y seguimiento de cuantas tareas y actividades sean precisas en el ámbito de la ciberseguridad, estableciendo las decisiones necesarias para satisfacer los requisitos de seguridad de la información y de los servicios, y proteger todos los activos en cualquier entidad, empresa, organización o administración pública.

Relación de módulos de formación

Módulo 1	CONCEPTOS CLAVE PARA EL GOBIERNO Y LA GESTIÓN DE LA SEGURIDAD	30 horas
Módulo 2	ANÁLISIS Y GESTIÓN DEL RIESGO	25 horas
Módulo 3	NORMATIVA, ESTÁNDARES, BUENAS PRÁCTICAS Y CUMPLIMIENTO LEGAL	20 horas
Módulo 4	GESTIÓN DE INCIDENTES, CRISIS Y CONTINUIDAD DE NEGOCIO	30 horas
Módulo 5	ARQUITECTURA Y OPERATIVA DE CIBERSEGURIDAD	30 horas
Módulo 6	SISTEMAS INDUSTRIALES E INFRAESTRUCTURAS CRÍTICAS	15 horas

Modalidades de impartición

Presencial
Teleformación

Duración de la formación

Duración total en cualquier modalidad de impartición	150 horas
Teleformación	Duración total de las tutorías presenciales: 0 horas

Requisitos de acceso del alumnado

Acreditaciones / titulaciones	Cumplir como mínimo alguno de los siguientes requisitos: -Título de Técnico Superior (FP Grado superior) o equivalente -Certificado de profesionalidad de nivel 3 -Título de Grado o equivalente

Acreditaciones / titulaciones	-Título de Postgrado (Máster) o equivalente
Experiencia profesional	No se requiere
Otros	- Conocimientos de nivel básico en temas de ciberseguridad. - Conocimientos de nivel básico-medio en informática a nivel de usuario. - Destrezas suficientes para utilizar una plataforma virtual en la que se apoya la acción formativa. En caso de no disponer de la titulación requerida, se realizará una prueba de competencias básicas suficientes para seguir el curso con aprovechamiento.
Modalidad de teleformación	Además de lo indicado anteriormente, los participantes han de tener las destrezas suficientes para ser usuarios de la plataforma virtual en la que se apoya la acción formativa.

Justificación de los requisitos del alumnado

- Para acreditar los requisitos de formación, se documentará con la presentación de los títulos o certificados correspondientes.

- Además el Centro deberá comprobar mediante una prueba de acceso que el candidato posee conocimientos generales relacionados con la especialidad indicados anteriormente.

Prescripciones de formadores y tutores

Acreditación requerida	Cumplir como mínimo alguno de los siguientes requisitos: - Licenciado, Ingeniero, Diplomado, Ingeniero Técnico, Técnico Superior relacionado con la especialidad. - Máster Universitario en Protección de Datos, Seguridad de la Información o Ciberseguridad.
Experiencia profesional mínima requerida	Experiencia profesional de un año en ocupaciones relacionadas con la especialidad objeto de contratación.
Competencia docente	- Certificado de profesionalidad de Docencia de la Formación Profesional para el Empleo o equivalente, o tener formación en metodología didáctica para adultos (mínimo 300 horas). - Experiencia docente de, al menos, 150 horas de impartición de formación en especialidades relacionadas con la especialidad objeto de contratación. - Titulaciones universitarias de Psicología/ Pedagogía/ o Psicopedagogía, Máster Universitario de Formación de Formadores u otras acreditaciones oficiales equivalentes.

Competencia docente	
Modalidad de teleformación	Además de cumplir con las prescripciones establecidas anteriormente, los tutores-formadores deben acreditar una formación, de al menos 30 horas, o experiencia, de al menos 60 horas, en esta modalidad y en la utilización de las tecnologías de la información y comunicación.

Justificación de las prescripciones de formadores y tutores

Para acreditar tanto los requisitos de formación como de experiencia impartiendo formación en las horas mínimas estipuladas, se documentará con la presentación de títulos y certificados oficiales, vida laboral, certificados de empresa o contratos más liquidación (que demuestre que se han ejecutado).

Requisitos mínimos de espacios, instalaciones y equipamientos

Espacios formativos	Superficie m² para 15 participantes	Incremento Superficie/ participante (Máximo 30 participantes)
Aula de gestión	45.0 m²	2.4 m² / participante

Espacio formativo	Equipamiento
Aula de gestión	- Mesa y silla para el formador - Mesas y sillas para el alumnado - Material de aula - Pizarra - PC instalado en red con posibilidad de impresión de documentos, cañón con proyección e Internet para el formador - PCs instalados en red e Internet con posibilidad de impresión para los participantes - Software específico para el aprendizaje de cada acción formativa. - Paquete integrado de ofimática. - Visor de documentos en formato pdf.

La superficie de los espacios e instalaciones estarán en función de su tipología y del número de participantes. Tendrán como mínimo los metros cuadrados que se indican para 15 participantes y el equipamiento suficiente para los mismos.

En el caso de que aumente el número de participantes, hasta un máximo de 30, la superficie de las aulas se incrementará proporcionalmente (según se indica en la tabla en lo relativo a m²/participante) y el equipamiento estará en consonancia con dicho aumento.

No debe interpretarse que los diversos espacios formativos identificados deban diferenciarse necesariamente mediante cerramientos.

Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico-sanitaria correspondiente y responderán a medidas de accesibilidad y seguridad de los participantes.

En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

Aula virtual

Características
• La impartición de la formación mediante aula virtual se ha de estructurar y organizar de forma que se garantice en todo momento que exista conectividad sincronizada entre las personas formadoras y el alumnado participante así como bidireccionalidad en las comunicaciones. • Se deberá contar con un registro de conexiones generado por la aplicación del aula virtual en que se identifique, para cada acción formativa desarrollada a través de este medio, las personas participantes en el aula, así como sus fechas y tiempos de conexión.
Otras especificaciones
Garantizar el soporte técnico permanente durante el horario docente del curso por parte del centro.

Para impartir la formación en **modalidad de teleformación**, se ha de disponer del siguiente equipamiento.

Plataforma de teleformación

La plataforma de teleformación que se utilice para impartir acciones formativas deberá alojar el material virtual de aprendizaje correspondiente, poseer capacidad suficiente para desarrollar el proceso de aprendizaje y gestionar y garantizar la formación del alumnado, permitiendo la interactividad y el trabajo cooperativo, y reunir los siguientes requisitos técnicos de infraestructura, software y servicios:

- **Infraestructura:**

  Tener un rendimiento, entendido como número de alumnos que soporte la plataforma, velocidad de respuesta del servidor a los usuarios, y tiempo de carga de las páginas Web o de descarga de archivos, que permita:

a) Soportar un número de alumnos equivalente al número total de participantes en las acciones formativas de formación profesional para el empleo que esté impartiendo el centro o entidad de formación, garantizando un hospedaje mínimo igual al total del alumnado de dichas acciones, considerando que el número máximo de alumnos por tutor es de 80 y un número de usuarios

b) Disponer de la capacidad de transferencia necesaria para que no se produzca efecto retardo en la comunicación audiovisual en tiempo real, debiendo tener el servidor en el que se aloja la plataforma un ancho de banda mínimo de 300 Mbs,

Estar en funcionamiento 24 horas al día, los 7 días de la semana.

- **Software:**

- Compatibilidad con el estándar SCORM y paquetes de contenidos IMS.

- Niveles de accesibilidad e interactividad de los contenidos disponibles mediante tecnologías web que como mínimo cumplan las prioridades 1 y 2 de la Norma UNE 139803:2012 o posteriores actualizaciones, según lo estipulado en el capítulo III del Real Decreto 1494/2007, de 12 de noviembre.

- El servidor de la plataforma de teleformación ha de cumplir con los requisitos establecidos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por lo que el responsable de dicha plataforma ha de identificar la localización física del servidor y el cumplimento de lo establecido sobre transferencias internacionales de datos en los artículos 40 a 43 de la citada Ley Orgánica 3/2018, de 5 de diciembre, así como, en lo que resulte de aplicación, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas respecto del tratamiento de datos personales y la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

- Compatibilidad tecnológica y posibilidades de integración con cualquier sistema operativo, base de datos, navegador de Internet de los más usuales o servidor web, debiendo ser posible utilizar las funciones de la plataforma con complementos (plug-in) y visualizadores compatibles. Si se requiriese la instalación adicional de algún soporte para funcionalidades avanzadas, la plataforma debe facilitar el

- Disponibilidad del servicio web de seguimiento (operativo y en funcionamiento) de las acciones formativas impartidas, conforme al modelo de datos y protocolo de transmisión establecidos en el anexo V de la Orden/TMS/369/2019, de 28 de marzo.

- **Servicios y soporte:**

- Sustentar el material virtual de aprendizaje de la especialidad formativa que a través de ella se imparta.

- Disponibilidad de un servicio de atención a usuarios que de soporte técnico y mantenga la infraestructura tecnológica y que, de forma estructurada y centralizada, atienda y resuelva las consultas e incidencias técnicas del alumnado. Las formas de establecer contacto con este servicio, que serán mediante teléfono y mensajería electrónica, tienen que estar disponibles para el alumnado desde el inicio hasta la finalización de la acción formativa, manteniendo un horario de funcionamiento de mañana y de tarde y un tiempo de demora en la respuesta no

- Personalización con la imagen institucional de la administración laboral correspondiente, con las pautas de imagen corporativa que se establezcan.

Con el objeto de gestionar, administrar, organizar, diseñar, impartir y evaluar acciones formativas a través de Internet, la plataforma de teleformación integrará las herramientas y recursos necesarios a tal fin, disponiendo, específicamente, de

- Comunicación, que permitan que cada alumno pueda interaccionar a través del navegador con el tutor-formador, el sistema y con los demás alumnos. Esta comunicación electrónica ha de llevarse a cabo mediante herramientas de comunicación síncronas (aula virtual, chat, pizarra electrónica) y asíncronas (correo electrónico, foro, calendario, tablón de anuncios, avisos). Será obligatorio que cada acción formativa en modalidad de teleformación disponga, como mínimo, de un servicio de mensajería, un foro y un chat.
- Colaboración, que permitan tanto el trabajo cooperativo entre los miembros de un grupo, como la gestión de grupos. Mediante tales herramientas ha de ser posible realizar operaciones de alta, modificación o borrado de grupos de alumnos, así como creación de «escenarios virtuales» para el trabajo cooperativo de los miembros de un grupo (directorios o «carpetas» para el intercambio de archivos, herramientas para la publicación de los contenidos, y foros o chats

- Administración, que permitan la gestión de usuarios (altas, modificaciones, borrado, gestión de la lista de clase, definición, asignación y gestión de permisos, perfiles y roles, autenticación y asignación de niveles de seguridad) y

- Gestión de contenidos, que posibiliten el almacenamiento y la gestión de archivos (visualizar archivos, organizarlos en carpetas –directorios- y subcarpetas, copiar, pegar, eliminar, comprimir, descargar o cargar archivos), la publicación organizada y selectiva de los contenidos de dichos archivos, y la

- Evaluación y control del progreso del alumnado, que permitan la creación, edición y realización de pruebas de evaluación y autoevaluación y de actividades y trabajos evaluables, su autocorrección o su corrección (con retroalimentación), su calificación, la asignación de puntuaciones y la ponderación de las mismas, el registro personalizado y la publicación de calificaciones, la visualización de información estadística sobre los resultados y el progreso de cada alumno y la obtención de informes de seguimiento.

Material virtual de aprendizaje:

El material virtual de aprendizaje para el alumnado mediante el que se imparta la formación se concretará en el curso completo en formato multimedia (que mantenga una estructura y funcionalidad homogénea), debiendo ajustarse a todos los elementos de la programación (objetivos y resultados de aprendizaje) de este programa formativo que figura en el Catálogo de Especialidades Formativas y cuyo contenido

- Como mínimo, ser el establecido en el citado programa formativo del Catálogo de Especialidades Formativas.

- Estar referido tanto a los objetivos como a los conocimientos/ capacidades cognitivas y prácticas, y habilidades de gestión, personales y sociales, de manera que en su conjunto permitan conseguir los resultados de aprendizaje

- Organizarse a través de índices, mapas, tablas de contenido, esquemas, epígrafes o titulares de fácil discriminación y secuenciase pedagógicamente de tal manera que permiten su comprensión y retención.

- No ser meramente informativos, promoviendo su aplicación práctica a través de actividades de aprendizaje (autoevaluables o valoradas por el tutor-formador) relevantes para la adquisición de competencias, que sirvan para verificar el progreso del aprendizaje del alumnado, hacer un seguimiento de sus dificultades

- No ser exclusivamente textuales, incluyendo variados recursos (necesarios y relevantes), tanto estáticos como interactivos (imágenes, gráficos, audio, video, animaciones, enlaces, simulaciones, artículos, foro, chat, etc.). de forma

- Poder ser ampliados o complementados mediante diferentes recursos adicionales a los que el alumnado pueda acceder y consultar a voluntad.

- Dar lugar a resúmenes o síntesis y a glosarios que identifiquen y definan los términos o vocablos básicos, relevantes o claves para la comprensión de los

- Evaluar su adquisición durante y a la finalización de la acción formativa a través de actividades de evaluación (ejercicios, preguntas, trabajos, problemas, casos, pruebas, etc.), que permitan medir el rendimiento o desempeño del alumnado.

Ocupaciones y puestos de trabajo relacionados

- ESPECIALISTA EN INCIDENCIAS DE SEGURIDAD
- RESPONSABLE DE LA SEGURIDAD CORPORATIVA Y EQUIPO DE TRABAJO (CSO CHIEF SECURITY OFFICER)
- RESPONSABLE DE SEGURIDAD DE SERVICIOS O PRODUCTOS TIC DE EMPRESAS PROVEEDORAS DE INFRAESTRUCTURAS CRÍTICAS O DE SERVICIOS ESENCIALES (ALCANCE DE LA LEY 40/2015), Y EQUIPO DE TRABAJO
- DIRECTOR DE CIBERSEGURIDAD (CISO CHIEF INFORMATION SECURITY OFFICER)
- RESPONSABLE DE LA SEGURIDAD DEL ESQUEMA NACIONAL DE SEGURIDAD (ART. 11 Y 13 DEL RD 311/2022)
- RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN (ART. 7 DEL RD 43/2021), Y EQUIPO DE TRABAJO
- ANALISTA DE SEGURIDAD
- RESPONSABLE DE CIBERSEGURIDAD, Y EQUIPO DE TRABAJO
- RESPONSABLE DE SEGURIDAD Y ENLACE DE LAS INFRAESTRUCTURAS CRÍTICAS (ART. 16 DE LA LEY 8/2011)
- ARQUITECTO DE SEGURIDAD, PARA LLEVAR A CABO EL PLAN DE CIBERSEGURIDAD A NIVEL TÉCNICO

Requisitos oficiales de las entidades o centros de formación

Estar inscrito en el Registro de entidades de formación (Servicios Públicos de Empleo).

Centro Móvil

Es posible impartir esta especialidad en centro móvil.

DESARROLLO MODULAR

MÓDULO DE FORMACIÓN 1:	**CONCEPTOS CLAVE PARA EL GOBIERNO Y LA GESTIÓN DE LA SEGURIDAD**

OBJETIVO

Identificar los puntos clave dentro de la Estrategia de Gestión de la Ciberseguridad para las Organizaciones, estándares, estrategia, política de ciberseguridad, gestión, auditorías y terceras partes.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 30 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- La Estrategia Nacional de Ciberseguridad.

- Objetivos, líneas de trabajo, y órganos de gobierno.

- Introducción y gestión de ciberseguridad.

- Qué es la ciberseguridad, fundamentos y marcos de control.

• Consideraciones generales sobre los sistemas de gestión.

- Sistemas de gestión de seguridad, ISO.

• Arquitecturas de seguridad.

- Introducción a la arquitectura de seguridad y su diseño, gestión, estrategias y principios.

• Sistemas de gestión de seguridad de la información aplicados sobre sistemas de información.

- Modelos organizativos, de relaciones, competencias vs capacidades.

• El responsable de seguridad de la información.

- Estrategia de seguridad, gobierno de ciberseguridad, competencias y capacidades, softskills.

• Certificaciones y acreditaciones.

- Requerimientos de seguridad, cláusulas de seguridad, acuerdos de nivel de servicio (SLAs), ISO/IEC 27001, 27002, Esquema Nacional de Seguridad (ENS), Informes de auditoría, evaluaciones y calificaciones, normativa y certificación en la nube.

• Ciberejercicios y plataformas de simulación.

- Motivación, tipología, marco de ejecución y puesta en valor, ciberejercicios de la Agencia de Ciberseguridad de la Unión Europea –ENISA, ciberejercicios del Instituto Nacional de Ciberseguridad de España - INCIBE, de la Oficina de Coordinación de Ciberseguridad - OCC y sectoriales.

• Cumplimiento y auditoría.

- Gestión del marco de control, marcos de control de la seguridad, matrices de controles con mapeo de estándares, regulaciones y marcos de referencia, Auditorías internas y externas. Evaluación de seguridad en el ENS.

• Concienciación, formación y capacitación del personal.

- Concienciación y sensibilización de empleados y directivos, formación y capacitación de los equipos de seguridad.

• Cadena de suministro.

- Particularidades de los servicios externalizados respecto al ENS, soluciones cloud y on-premise, contratación y seguimiento acuerdos con proveedores, seguridad

desde el diseño.

Habilidades de gestión, personales y sociales

- Interés por la seguridad de la información y la tecnología.

- Concienciación de los riesgos de seguridad informática y de la importancia de aplicar políticas y medidas técnicas y organizativas a fin de prevenir las ciberamenazas.

MÓDULO DE FORMACIÓN 2: ANÁLISIS Y GESTIÓN DEL RIESGO

OBJETIVO

Detectar posibles amenazas a la organización en materia de ciberseguridad, identificando los riesgos para poder valorarlos, gestionarlos y tratarlos apropiadamente en función a su peligrosidad, principales amenazas tecnológicas y gestión de riesgos en Ciberseguridad.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 25 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Riesgos de seguridad.

- Modelo de gestión de riesgos, análisis de riesgos, controles de seguridad, plan de acción, reporte de riesgos, cuadros de mando.

- Identificación de activos y marco regulatorio.

- Identificación y tipologías de activos.

- Vulnerabilidades, amenazas, probabilidades e impactos.

- Definición de conceptos y evaluación del riesgo.

- Análisis de riesgos.

- Riesgos de ciberseguridad, riesgos corporativos, identificación y evolución de fuentes de amenaza, apetito de riesgo de seguridad.

- Gestión y tratamiento de riesgos de seguridad.

- Programas de tratamiento, estrategias.

- Estrategias especiales para el tratamiento de riesgos de seguridad.

- Riesgos de terceros, amenazas híbridas y desinformación, ciberseguros, teletrabajo.

Habilidades de gestión, personales y sociales

- Análisis crítico de la estructura de seguridad de la organización.

- Seleccionar las formas de protegerse y proteger a los demás en riesgos para la salud y amenazas físicas y psicológicas en relación al uso de las tecnologías digitales.

MÓDULO DE FORMACIÓN 3: NORMATIVA, ESTÁNDARES, BUENAS PRÁCTICAS Y CUMPLIMIENTO LEGAL

OBJETIVO

Garantizar el cumplimiento legal en materia de ciberseguridad de la organización ante los estamentos correspondientes, utilizando herramientas de gestión del cumplimiento estándares y marcos de control nacionales e internacionales, regulaciones y Leyes, Cibercrimen, Infraestructuras Críticas, la prueba digital.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 20 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Cumplimiento.

- Organización y protocolos internos, análisis y gestión de riesgos de cumplimiento y planes de acción, figuras y roles en el cumplimiento, seguimiento, evaluación y auditoría.

- Requerimientos legales y regulatorios.

- Regulación nacional e internacional (ENS, NIS, NIS2, RGPD, LPIC, eIDAS), regulaciones sectoriales.

• Estándares y marcos de control nacionales e internacionales.

- Estándares, marcos de referencia y mejores prácticas (ISO, UNE, ENS, NIST, SANS, COBIT, UIT, NATO).

• Diferentes sistemas de gestión de la seguridad legales y normativos.

- ENS, UNE ISO/IEC 27001:2022 Sistemas de Gestión de Seguridad de la Información (SGSI), certificaciones cloud, ISO 22301:2019 Sistemas de Gestión de Continuidad del Negocio (SGCN).

• Aspectos legales del Cibercrimen y delitos informáticos.

- Recogida, preservación, presentación y custodia de indicios y evidencias electrónicas, regulación del Código Penal, investigaciones ante el Cibercrimen, aspectos jurisdiccionales y normativa aplicable.

Habilidades de gestión, personales y sociales

• Habilidad para definir estrategias para la Gestión y tratamiento de Riesgos de Seguridad, siendo capaces de realizar un análisis de cumplimiento, diferenciando la situación actual, la situación objetivo y la situación óptima.

• Detección de los impactos medioambientales de las tecnologías digitales y su protección.

MÓDULO DE FORMACIÓN 4:	GESTIÓN DE INCIDENTES, CRISIS Y CONTINUIDAD DE NEGOCIO

OBJETIVO

Supervisar la gestión de la ciberseguridad de la organización, estando preparados para articular la respuesta y la recuperación de la información ante un ciberataque, coordinando y llevando a cabo el seguimiento de las decisiones adoptadas, detección, tratamiento, análisis y notificación de brechas. Continuidad y Resiliencia.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 30 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Planificación de una gestión de Crisis.

- Definición del Plan de crisis, roles y responsabilidades, fases y decisiones, comunicación, mecanismos, toma de decisiones, impactos, reguladores, planes de acción y recuperación, simulacros y simulaciones, presupuesto, plan de continuidad.

- Gestión de brechas e incidentes de seguridad.

- Incidentes e incidencias, detección, registro y documentación, estrategias de investigación, escalado, análisis, recuperación, estrategias de minimización de situaciones de riesgo, lecciones aprendidas.

- Notificación de incidentes y violaciones de seguridad.

- Regulación, autoridades de control, acciones legales y judiciales, límites legales en la investigación, responsabilidad legal, notificación de brechas de seguridad y violaciones de datos.

- CERT/CSIRT y SOC.

- Estructura, funciones, intercambio de información, indicadores de compromiso.

- Análisis forense y búsqueda de evidencias.

- Visión general del análisis forense, metodologías, ciclo de vida de un incidente, cadena de custodia, adquisición de evidencias, clonado, herramientas.

- Gestión de Crisis y Continuidad de Negocio.

- Planes, protocolos, ubicaciones, comités de crisis, roles, comunicación, responsables, mando y control, herramientas, coordinación y cooperación, toma de decisiones, monitorización, informes y lecciones aprendidas.

Habilidades de gestión, personales y sociales

- Toma de medidas de protección de los datos empresariales, personales, y la privacidad ante daños y peligros digitales.

- Diferenciación entre el concepto de Planes de Continuidad de Negocio (PCN), los Análisis de Impacto en el Negocio (BIA) y las herramientas de seguimiento, evaluación y auditoría de seguridad.

MÓDULO DE FORMACIÓN 5: ARQUITECTURA Y OPERATIVA DE CIBERSEGURIDAD

OBJETIVO

Prevenir y asesorar en el diseño de una operativa de ciberseguridad que contemple los aspectos principales orientándolos a las características específicas de la organización: Tecnologías, Herramientas, Servicios y Capacidades, Infraestructura de seguridad, pentesting, monitorización, gestión de vulnerabilidades, respuesta, desarrollo seguro, etc.

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 30 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- Operaciones de ciberseguridad.

- Identificar, proteger, detectar, responder y recuperar.

- Arquitectura y tecnologías de la ciberseguridad.

- Tipologías de arquitectura (On-premise/Cloud), protección de la información, protección de sistemas y servicios, protección de la infraestructura y redes, protección de dispositivos móviles.

- Monitorización y detección.

- Conceptos esenciales, casos de uso, MITRE, SOC Security Operation Centre.

- Información de seguridad y gestión de eventos (SIEM).

- Capacidades de un SIEM (Security Information and Event Management), ventajas de la monitorización de sistemas.

- Análisis y gestión de vulnerabilidades.

- Tipologías de vulnerabilidades, gestión, detección, metodologías y herramientas de análisis y gestión.

- Análisis y gestión de malware.

- Estado actual, familias y tipos, herramientas y técnicas de análisis, laboratorio de malware.

- APT Amenazas Persistentes Avanzadas.

- Concepto, infección, mecanismos de protección, soluciones anti-APT.

- Pruebas técnicas Hacking ético y auditorías técnicas.

- Objetivos, definición y terminología, técnicas y metodologías, pentesting, MITRE ATT@CK, NIST, OWASP (Open Web Application Security Project), tipología de pruebas, herramientas.

- Ciberinteligencia y cooperación.

- Ciclo de ciberinteligencia y fuentes internas y externas, relaciones con organismos nacionales e internacionales (CCN-CERT, INCIBE-CERT, ESPDEF-CERT, ENISA, FS-ISAC, FIRST), intercambio de información de inteligencia.

- Desarrollo seguro.

- Introducción, objetivos, conceptos y definiciones, referencias metodológicas y normativas, ciclo de vida de desarrollo de software seguro.

- Criptografía.

- Introducción, objetivos, conceptos y definiciones, tipos de criptografía, procedimientos de gestión y custodia de claves, mecanismos criptográficos, PKI (Public Key Infrastructure), HSM (Hardware Security Module), técnicas de ofuscación.

Habilidades de gestión, personales y sociales

- Elección de medidas para proteger dispositivos y contenidos digitales a partir de sus riesgos y amenazas en entornos digitales, teniendo en cuenta la fiabilidad y privacidad.

- Interpretación y comunicación de las necesidades de seguridad de la organización ante el equipo informático ejecutor de la prevención y la dirección de la organización.

MÓDULO DE FORMACIÓN 6:	SISTEMAS INDUSTRIALES E INFRAESTRUCTURAS CRÍTICAS

OBJETIVO

Escalar los sistemas de gestión de seguridad estudiados a entornos industriales, e infraestructuras críticas, ciberseguridad específica en los sistemas industriales e infraestructuras críticas (IOT-Internet of Things).

DURACIÓN EN CUALQUIER MODALIDAD DE IMPARTICIÓN: 15 horas

Teleformación: Duración de las tutorías presenciales: 0 horas

RESULTADOS DE APRENDIZAJE

Conocimientos / Capacidades cognitivas y prácticas

- La Ciberseguridad Industrial. IoT, IIoT, OT Operational Technology.

- Concepto, similitudes y diferencias, estándar ISA99 / IEC 62443.
- Sistemas de protección de infraestructuras críticas.Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).

- Operadores críticos y servicios esenciales. Modelo de colaboración público-privada.

- La Oficina de Coordinación de Ciberseguridad (OCC).
- La Agencia de Ciberseguridad de la Unión Europea –ENISA.
- Los CERT Computer Emergency Response Team de referencia (CCN-CERT, INCIBE-CERT).
- La Plataforma Tecnológica Española de Seguridad Industrial – PESI.
- El Centro de Ciberseguridad Industrial (CCI).

Habilidades de gestión, personales y sociales

- Detección del riesgo en seguridad cibernética de infraestructuras críticas y servicios esenciales tanto en la industria como en organizaciones clave.

- Gestión proactiva de la seguridad cibernética en infraestructuras críticas y

servicios esenciales tanto en la industria como en organizaciones clave.

ORIENTACIONES METODOLÓGICAS

Esta Formación está diseñada preferentemente para ser impartida en modalidad presencial o en Aula Virtual.

El enfoque didáctico debe combinar la asimilación del marco conceptual de la disciplina, su aplicabilidad en casos de éxito y ejercicios participativos individuales y en grupo, haciendo del programa una experiencia real, dinámica, práctica y rica en experiencias.

Esta formación debe desarrollarse de forma práctica fomentando permanentemente la colaboración y el debate entre los participantes.

Para alcanzar los resultados óptimos de aprendizaje que se recogen en el módulo 2 de Análisis y gestión del riesgo se propone la implementación sobre un supuesto práctico del estándar ISO 31000 Directrices para la Gestión de Riesgos aplicando los principios, marco de referencia y proceso a seguir.

Para alcanzar los resultados de aprendizaje que se recogen en el módulo 6 se propone completarlos con la realización de un trabajo, individual o en grupo, de implementación del estándar IEC 62443 en un supuesto práctico.

Se aportarán a los alumnos los materiales tanto en formato digital como físico para ayudar al estudio y preparación de las evaluaciones y certificaciones.

Se apoyará el contenido de las clases con un aula virtual que tiene como objetivo servir de repositorio de documentación, facilitar la realización de las evaluaciones y potenciar la comunicación con los alumnos.

EVALUACIÓN DEL APRENDIZAJE EN LA ACCIÓN FORMATIVA

- La evaluación tendrá un carácter teórico-práctico y se realizará de forma sistemática y continua, durante el desarrollo de cada módulo y al final del curso.
- Puede incluir una evaluación inicial de carácter diagnóstico para detectar el nivel de partida del alumnado.
- La evaluación se llevará a cabo mediante los métodos e instrumentos más adecuados para comprobar los distintos resultados de aprendizaje, y que garanticen la fiabilidad y validez de la misma.
- Cada instrumento de evaluación se acompañará de su correspondiente sistema de corrección y puntuación en el que se explicite, de forma clara e inequívoca, los criterios de medida para evaluar los resultados alcanzados por los participantes.
- La puntuación final alcanzada se expresará en términos de Apto/ No Apto.