GUÍA DIDÁCTICA DE LA CERTIFICACIÓN EN CIBERSEGURIDAD

- Certificación emitida por Bureau Veritas
- Proceso gestionado por FIBSEM

1. Presentación de la Certificación

La Certificación en Ciberseguridad acredita los conocimientos, competencias y habilidades profesionales necesarias para diseñar, implementar y gestionar sistemas de seguridad informática, proteger infraestructuras críticas digitales, afrontar incidentes cibernéticos y garantizar la continuidad del negocio ante ciberataques.

Está dirigida a profesionales como Responsables de Seguridad de la Información, CISO, Analistas de Ciberseguridad, Ingenieros de Seguridad, Incident Response Managers, Consultores de TI, y otros perfiles implicados en protección digital y estrategia corporativa.

2. Objetivos Generales

- Capacitar al profesional en los fundamentos de la ciberseguridad (confidencialidad, integridad, disponibilidad, autenticación, no repudio).
- Identificar y analizar amenazas y vulnerabilidades en entornos digitales, tanto técnicas como de gestión.
- Proteger infraestructuras críticas digitales, garantizando su resiliencia ante ataques.
- Implementar medidas de seguridad informática (control de accesos, criptografía, redes, protocolos, monitorización).
- Gestionar de forma eficiente los incidentes cibernéticos, desde la detección hasta la recuperación.
- Conocer y aplicar criptografía y protección de datos en entornos corporativos.
- Alinear la estrategia de ciberseguridad con normativas internacionales.
- Gestionar la seguridad en redes y accesos, garantizando controles robustos frente a amenazas externas e internas.
- Diseñar planes de resiliencia y continuidad del negocio ante ciberataques, asegurando que la organización pueda recuperarse de forma ágil.

3. Proceso de Certificación

Fase 1. Revisión del curriculum y documentación

El candidato debe presentar su solicitud de certificación a FIBSEM, incluyendo:

- Curriculum Vitae actualizado.
- Copia de titulaciones/certificados relacionados con seguridad informática, ciberseguridad, redes, análisis de vulnerabilidades o gestión de riesgos digitales.
- Justificante de experiencia profesional en el campo de la ciberseguridad o TI (se recomienda mínimo 2 años).

El responsable de FIBSEM en la región del candidato:

1. Verifica la documentación y experiencia profesional.
2. Emite un informe de elegibilidad.
3. Autoriza el acceso al itinerario formativo correspondiente.

Fase 2. Itinerario Formativo

Una vez validada la documentación, el candidato recibe acceso a la plataforma o itinerario (online/presencial) donde completará los módulos formativos necesarios para preparar la certificación.

Fase 3. Evidencia de competencias

Durante el itinerario formativo o al finalizar este, el candidato deberá aportar evidencias prácticas que demuestren su competencia profesional.

Estas evidencias serán revisadas por el equipo académico de FIBSEM.

Evidencias requeridas:

1. Análisis de vulnerabilidades en un entorno digital real o simulado, acompañado de propuesta de soluciones.
2. Simulación de un ataque cibernético y desarrollo de la estrategia de respuesta (detección, contención, erradicación, recuperación).
3. Desarrollo de un plan de seguridad digital basado en normativas internacionales (ISO 27001, NIST) y buenas prácticas.

Criterios de evaluación:

- Coherencia técnica.

- Aplicación normativa.
- Estructura y presentación profesional.

Fase 4. Examen de Certificación (Bureau Veritas)

Una vez completados los itinerarios formativos y validadas las evidencias, el candidato podrá inscribirse en las convocatorias oficiales de examen gestionadas por Bureau Veritas.

Características del examen:

- Modalidad: Online supervisada.
- Duración: 90 minutos.
- Tipo de prueba: test de 60 preguntas + caso práctico.
- Criterio de aprobación: 70 % mínimo.

Al superar el examen, el candidato obtendrá la **Certificación en Ciberseguridad IBEROSEC**, con validez internacional.

4. Metodología Didáctica

- Aprendizaje autónomo y tutorizado mediante recursos multimedia, lecturas, vídeos y foros.
- Casos prácticos reales o simulados (ataques, incidentes, recuperación) que permiten aplicar el conocimiento técnico y de gestión.
- Evaluaciones progresivas al final de cada módulo.
- Laboratorios o simulaciones en entorno controlado para aplicar medidas técnicas (por ejemplo, análisis de vulnerabilidad, respuesta a incidentes).
- Tutorías personalizadas con expertos certificados.

5. Recursos Didácticos

- Plataforma virtual FIBSEM (manuales PDF, vídeos, test, foros)
- Manual del participante.
- Documentación de referencia: artículos, normas, marcos de ciberseguridad (por ejemplo, NIST CSF y ISO 27001)
- Plantillas editables: análisis de vulnerabilidad, plan de respuesta a incidentes, plan de implementación de ISMS, matriz de riesgos digitales.

6. Criterios de Evaluación Global

Para la obtención de la certificación, el candidato deberá superar el examen de certificación, previa aprobación de pre-requisitos y de las pruebas teóricas por modulo y el caso practico final.