TABLA 11: Unidades de Aprendizaje

(Una por cada Unidad)

Unidad de Aprendizaje Nº 1 **Plan de prevención y concienciación en ciberseguridad**		
Temporalización: Semana 1ª-6ª	**Duración**: 30 horas	**Ponderación**: 20%

Objetivos Generales	Competencias
a) Identificar los principios de la organización y normativa de protección en ciberseguridad planificando las acciones que es preciso adoptar en el puesto de trabajo para la elaboración del plan de prevención y concienciación. **b) Auditar el cumplimiento del plan de prevención y concienciación de la organización definiendo las acciones correctoras que puedan derivarse para incluirlas en el plan se securización de la organización.**	**a) Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización aplicando la normativa vigente.** **b) Detectar e investigar incidentes de ciberseguridad documentándolos e incluyéndolos en los planes de securización de la organización**
Resultados de Aprendizaje	
1. Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo	

normas y medidas de protección.	
Aspectos del Saber Hacer	**Aspectos del Saber**
Define los principios generales de ciberseguridad que debe tener una empresa.	Principios generales en materia de ciberseguridad. Normativa de protección del puesto del trabajo Plan de formación y concienciación en materia de ciberseguridad. Materiales de formación y concienciación. Auditorías internas de cumplimiento en materia de prevención.
Establece las politicas de seguridad necesarias para garantizar la seguridad informática en los lugares de trabajo.	
Desarrolla un plan de concienciación adaptado a la empresa.	
Elabora material de concienciación y ejecuta activiades de ingeniería social como *phishing* en el lugar de trabajo.	
Conoce la normativa referente a las auditorías, los tipos que existen, como se llevan a cabo y sabe aplicarlas.	
Aspectos del Saber Estar	
Valora el grado de aplicación de dicha normativa al contexto de la empresa.	
Tiene en cuenta el conocimiento en materia de ciberseguridad de la plantilla	

de cara a la elaboración del plan de concienciación.	
Pone en valor la realización periódica de una auditoría como método de mejorar de forma contínua el nivel de seguridad.	

Tareas y Actividades

- Se introducirán los conceptos más habituales relacionados con los incidentes de ciberseguridad
- Se introducirán diversos métodos de protección del puesto de trabajo y de la empresa.
- Se explicarán los conceptos relacionados con el phising.
- Se realizará una práctica de phising.
- Los alumnos presentarán un plan de concienciación para los trabajadores.

Criterios de Evaluación	%	IE
a) Se han definido los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección de la misma.	15	Examen teórico
b) Se ha establecido una normativa de protección del puesto de trabajo.	25	Presentación individual.
c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.	25	Presentación individual.
d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.	25	Práctica

e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.	10	Examen teórico

Recursos
Aula-taller con ordenadores para cada uno de los alumnos de la clase. Los equipos deberán contar con herramientas de ofimatica básicas, software de virtualización y suficiente memoria y disco duro como para poder virtualizar varias máquinas de forma rápìda. Una pantalla o proyector.
Observaciones

Unidad de Aprendizaje Nº 2 Identificación de incidentes de ciberseguridad		
Temporalización: Semanas 7ª-11ª	**Duración**: 25	**Ponderación**: 10%

Objetivos Generales	**Competencias**
Detectar incidentes de ciberseguridad implantando los controles, las herramientas y los mecanismos necesarios para su monitorización e identificación.	**Detectar e investigar incidentes de ciberseguridad documentándolos e incluyéndolos en los planes de securización de la organización.**
Resultados de Aprendizaje	

2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.

Aspectos del Saber Hacer	Aspectos del Saber
Conoce lo que es una taxonomía y ejemplos de ellas en el ámbito de la clasificación de incidentes de ciberseguridad. Implementa métodos de detección de incidentes basados en la monitorización de redes, losg, etc, empleando herramientas como un IDS o un SIEM. Conoce los riesgos de una baja seguridad física y desarrolla mecanismos para mejorarla. Automatiza el proceso de detección de incidentes haciendo uso de fuentes abiertas. Aplica la taxonomía para clasificar los incidentes y mantiene canales de comunicación, documentación y control de los mismos.	Taxonomía de incidentes de ciberseguridad Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes: tipos y fuentes Controles, herramientas y mecanismos de detección e identificación de incidentes de seguridad física Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT). Clasificación, valoración, documentación, seguimiento inicial de incidentes de ciberseguridad.
Aspectos del Saber Estar	

Valora la importancia de una taxonomía de calidad a la hora de trabajar con los diferentes incidentes. Reconoce el valor de los sistemas de detección y alerta de incidentes para la detección temprana y en pos de facilitar la mitigación posterior. Importancia de valorar la seguridad física y/o perimetral como un incidente o vector de ataque más de ciberseguridad. Reconoce la importancia de una gestión organizada de los incidentes entre todos los miembros de la organización.	

Tareas y Actividades

- Se va a mostrar una taxonomía general de los incidentes de ciberseguridad.
- Se van a utilizar diferentes herramientas para la monitorización y el control de las posibles incidencias. Se utilizarán SNORT, OpenVA, AlientVault... Se usarán sistemas operativos para correr estas aplicaciones o bien virtualización mediante contenedores. De estas herramientas se hará una pequeña introducción teórica de cada una y posteriormente una práctica.

Criterios de Evaluación	%	IE
a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización	10	Examen teórico
b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes	20	Práctica
c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física	30	Práctica
d) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT: *Open Source Intelligence*)	30	Práctica
e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.	10	Examen teórico

Recursos
Aula-taller con ordenadores para cada uno de los alumnos de la clase. Los equipos deberán contar con herramientas de ofimática básicas, software de virtualización y suficiente memoria y disco duro como para poder virtualizar varias máquinas de forma rápida. Una pantalla o proyector.

Observaciones

Unidad de Aprendizaje Nº 3 Investigación de incidentes de ciberseguridad

Temporalización: Semana 12ª-19ª	**Duración**: 40 h	**Ponderación**: 20%

Objetivos Generales	Competencias
d) Analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación. **r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.**	**b) Detectar e investigar incidentes de ciberseguridad documentándolos e incluyéndolos en los planes de securización de la organización.** **l) Adaptarse a las nuevas situaciones laborales manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.**

Resultados de Aprendizaje	
3. Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.	
Aspectos del Saber Hacer	**Aspectos del Saber**

Recopila las diferentes evidencias del incidente. Analiza las evidencias del incidente realizando una categorización inicial de su impacto y riesgo. Investiga el incidente para determinar las causas del mismo y conocer los servicios e información que se han visto afectados. Intercambia datos del incidente con otros organismos y entidades especializados en la ciberseguridad. Toma medidas de prevención antes de que otros equipos, sistemas o datos se vean afectados por el incidente.	Recopilación de evidencias. Análisis de evidencias. Investigación del incidente Intercambio de información del incidente con proveedores u organismos competentes. Medidas de contención de incidentes.
Aspectos del Saber Estar	
Es metodológico y ordenado a la hora de realizarlo.	

Tareas y Actividades

- Se van a utilizar herramientas para catalogar y gestionar las incidencias y *logs* que se detecten. Por ejemplo, se plantea el uso de una base de datos no relacional a través

del *stack ELK* para la gestión de múltiples fuentes de incidencia de forma centralizada y ágil.

- Se analizarán archivos sospechosos de forma estática, dinámica y mediante *reversing* de código de dichos archivos.

Criterios de Evaluación	%	IE
a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.	20	Práctica (50%) FEM (50%)
b) Se ha realizado un análisis de evidencias.	30	Práctica
c) Se ha realizado la investigación de incidentes de ciberseguridad	20	Práctica
d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto	10	Práctica
e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados	20	Cuestionario multirespuesta

Recursos

Aula-taller con ordenadores para cada uno de los alumnos de la clase.

Los equipos deberán contar con herramientas de ofimática básicas, software de virtualización y suficiente memoria y disco duro como para poder virtualizar varias máquinas de forma rápida.

Una pantalla o proyector.

Observaciones

Unidad de Aprendizaje Nº 4 Protección ante los incidentes de ciberseguridad		
Temporalización: Semana 20ª- 27ª	**Duración**: 35 h	**Ponderación**: 30%

Objetivos Generales	Competencias
s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal . **t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo para garantizar entornos seguros.** **u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».**	**m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.** **n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.** **ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en**

	las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

Resultados de Aprendizaje	
4. Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.	
Aspectos del Saber Hacer	**Aspectos del Saber**
Desarrolla procedimientos de gestión de incidentes para dar una respuesta rápida a aquellos más habituales o que pudieran tener un mayor impacto. Implementa desarrollos de software que permiten ofrecer el servicio pese a la existencia de un ciberataque con técnicas de replicación y distribución de contenidos y alta disponibilidad. Lleva a cabo todas las tareas de restauración del servicio eliminando los daños realizados por el incidente durante el proceso de recuperación. Documenta el proceso de resolución	Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes. Implantar capacidades de ciberresiliencia. Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados. Tareas para reestablecer los servicios afectados por incidentes. Documentación Seguimiento de incidentes para evitar una situación similar.

del incidente para su aprovechamiento en el futuro. Desarrolla planes de prevención y de recuperación en base a los errores del incidente para evitar o minimizar daños futuros.	
Aspectos del Saber Estar	
Asume su responsabilidad y toma las decisiones que le corresponden durante el incidente.	

Tareas y Actividades

- Se aplicarán técnicas de disuasión como los *honeypots* mediante prácticas en el aula.
- Se realizará una práctica de copias de seguridad remotas mediante el uso de bacula.
- Se configurará en una práctica una solución de ticketing que pueda implementarse para la gestión de incidentes.
- Se realizará un trabajo en el que se simule de forma grupal una restauración de un sistema tras un incidente.

Criterios de Evaluación	%	IE
a) Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.	20	Trabajo grupal (50%) FEM (50%)
b) Se han preparado respuestas ciberresilientes ante incidentes que permitan seguir prestando los servicios de la organización y	15	Trabajo grupal

fortaleciendo las capacidades de identificación, detección, prevención, contención, recuperación y cooperación con terceros.		
c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.	15	Trabajo grupal
d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.	15	Trabajo grupal
e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de "lecciones aprendidas".	20	Práctica
f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se repita.	15	Práctica

Recursos

Aula-taller con ordenadores para cada uno de los alumnos de la clase.

Los equipos deberán contar con herramientas de ofimática básicas, software de virtualización y suficiente memoria y disco duro como para poder virtualizar varias máquinas de forma rápida.

Una pantalla o proyector.

Observaciones

Unidad de Aprendizaje Nº 5

Documentación de incidentes de ciberseguridad.

Temporalización: Semana 28ª-33ª	**Duración**: 28 h	**Ponderación**:20%

Objetivos Generales	Competencias
q) Desarrollar manuales de información utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa. **v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calida.**	**k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente respondiendo a los requisitos establecido.** **ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.**

Resultados de Aprendizaje	
5. Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.	
Aspectos del Saber Hacer	**Aspectos del Saber**
Elabora un plan de actuación para la notificación del incidente.	

Mantiene canales de información y documentación a empleados y colaboradores de la empresa. Notifica por los canales adecuado y proporcionando la información necesaria la existencia de un incidente. Notifica el incidente a los afectados. Comunica el incidente en medios de comunicación si fuera necesario.	Desarrollar procedimientos de actuación para la notificación de incidentes. Notificación interna de incidentes. Notificación de incidentes a quienes corresponda Notificación de incidentes a quienes corresponda Notificación de incidentes a quienes corresponda
Aspectos del Saber Estar	
Tiene en cuenta la normativa vigente en materia de notificación de incidentes a los CERT que correspondan. Valora la importancia de la comunicación exterior de cara a la imagen de la empresa. Valora la importancia de la comunicación exterior de cara a la imagen de la empresa.	
Tareas y Actividades	

- Se realizará un trabajo especificando varios procesos de actuación para
- En el mismo trabajo se añadirá un plan de notificación interno y externo del incidente.

Criterios de Evaluación	%	IE
a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.	40	Trabajo individual (50%) FEM (50%)
b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.	15	Trabajo individual
c) Se ha notificado el incidente de manera adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.	15	Trabajo individual
d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.	15	Trabajo individual
e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.	15	Trabajo individual

Recursos

Aula-taller con ordenadores para cada uno de los alumnos de la clase.

Los equipos deberán contar con herramientas de ofimática básicas, software de virtualización y suficiente memoria y disco duro como para poder virtualizar varias máquinas de forma rápida.

Una pantalla o proyector.

Observaciones