Curso online de ciberseguridad

HOJA DE RUTA

El plan de Concienciación y Sensibilización también contempla la realización de una hoja de ruta en Ciberseguridad compuesto de seis (6) módulos de formación online, que proporcionará a sus alumnos los conocimientos necesarios para conseguir una concienciación adecuada para el correcto empleo de las tecnologías e impulsar, al mismo tiempo, el conocimiento de las amenazas y vulnerabilidades asociadas a su uso.

Los módulos que conformarán el programa son:

1. Módulo básico de ciberseguridad
2. Módulo de seguridad en correo electrónico
3. Módulo de navegación segura
4. Módulo de seguridad en dispositivos móviles
5. Módulo sobre amenazas: ransomware
6. Módulo de gestión de cibercrisis

Cada módulo formativo dispondrá de una fase teórica de 15 horas de duración y una fase práctica de la misma duración. En total, se dedicará a cada módulo un total de 30 horas de formación. La duración de cada módulo será de cuatro (4) semanas desde el inicio del proyecto. En total, la hoja de ruta en Ciberseguridad tendrá una duración de 180 horas de formación (24 semanas).

Antes del inicio del primer módulo, es decir, el primer día del curso, los alumnos serán convocados a una sesión en directo en la que se dará la bienvenida a los asistentes y se explicará el contenido y metodología del curso.

La metodología del curso, así como la definición y fases de cada módulo se describen en los siguientes epígrafes.

Metodología

El presente Plan de Concienciación y Sensibilización emplea una metodología docente 100% online, fomentando la formación teórico-práctica en materia de ciberseguridad. Asimismo, permitirá evaluar los conocimientos adquiridos por parte de los alumnos.

Cada uno de los seis (6) módulos de formación dispondrá de una fase teórica y de una fase práctica. A continuación se describen las distintas actividades que el alumno deberá realizar en cada una de las fases:

FASE TEÓRICA - 15 horas por módulo

En esta primera fase del curso, se proporcionará a los alumnos, a través de material interactivo, el contenido teórico del curso que versará sobre la temática establecida en cada módulo. Esta fase está compuesta de tres (3) tipos de actividades, que se llevarán a cabo siguiendo el orden que a continuación se indica:

- ✓ Vídeo introductorio: el alumno comenzará cada módulo de formación visionando un vídeo ya grabado en el que se hará una breve introducción al módulo del que se trate.
- ✓ Curso online: visionado el vídeo introductorio, el alumno realizará un curso online a través de ÁNGELES, el portal de formación capacitación y talento en ciberseguridad del Centro Criptológico Nacional.

  Mediante dicho curso se explicarán temáticas concretas en el ámbito de la ciberseguridad y se pondrá a disposición de los alumnos material formativo adicional y complementario al curso, con el que podrá profundizar en los contenidos de cada módulo.

  El alumno dispondrá de dos (2) semanas para realizar el curso online. Finalizada la fase de contenido teórico, el alumno deberá superar un examen de evaluación con nota de corte del 65%.
- ✓ Sesiones de formación en directo: en paralelo a la realización del curso online, y durante las dos (2) primeras semanas del módulo, el alumno asistirá a dos (2) sesiones de formación en directo, de entre 60 y 90 minutos de duración, que complementarán el contenido teórico del curso online.

FASE PRÁCTICA – 15 horas por módulo

Finalizadas las dos (2) primeras semanas del curso, y habiendo completado la fase teórica, el alumno pondrá a prueba los conocimientos adquiridos durante la segunda fase del curso: la fase práctica, que también tendrá dos (2) semanas de duración.

- ✓ Retos de ciberseguridad: para afianzar los conocimientos adquiridos, se emplearán las soluciones ATENEA, la plataforma de retos de ciberseguridad, y ELENA, simulador de cibervigilancia, del Centro Criptológico Nacional, a través de la cual el alumno tendrá que poner en práctica y a prueba, a través de distintos desafíos de seguridad, los conocimientos adquiridos en la fase teórica.
- ✓ Sesiones de formación en directo: en paralelo a la realización de los retos de ATENEA y ELENA, el alumno asistirá a dos (2) sesiones de formación en directo, de entre 60 y 90 minutos de duración.

Todo ello se complementará con un servicio de tutoría tipo blog, donde los alumnos podrán enviar por escrito preguntas, dudas y consultas a los expertos del curso sobre el contenido del material impartido en las diferentes fases.

1er Módulo

Módulo Básico de Ciberseguridad

1er mes 30 horas de formación

Se puede decir que no existe un sistema que garantice al 100% la seguridad del servicio que presta y la información que maneja debido, en gran medida, a las vulnerabilidades que presentan las tecnologías y lo que es más importante, la imposibilidad de disponer de los suficientes recursos para hacerlas frente.

Por tanto, siempre hay que aceptar un riesgo; el conocido como riesgo residual, asumiendo un compromiso entre el nivel de seguridad, los recursos disponibles y la funcionalidad deseada. Por ello, en este módulo se enseñarán las medidas fundamentales para mantener la seguridad en las Tecnologías de la Información y la Comunicación (TIC), abordando distintas temáticas como: amenazas en el ciberespacio, vectores de infección, deep web, seguridad en redes inalámbricas, IOT, mensajería instantánea y redes sociales, entre otras temáticas

El contenido del presente módulo será impartido durante cuatro (4) semanas, divididas en una fase teórica y en una fase práctica.

A continuación se indica la programación y plazos para la realización de las diferentes actividades programadas para este módulo:

- Sesión de directo de bienvenida y explicación del curso y módulos
- Introducción al módulo mediante vídeo grabado por los expertos
- Fase teórica: realización de curso online
- Sesión de formación en directo a través de zoom
- Examen de evaluación
- Fase práctica: retos de ciberseguridad ATENEA / ELENA

1er mes

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
1ª semana	Sesión en directo. Bienvenida y explicación del curso	Fase teórica: Curso online Básico de Ciberseguridad en ÁNGELES Vídeo introductorio del módulo			Sesión en directo (2 hrs)		
2ª semana	Fase teórica: Curso online Básico de Ciberseguridad en ÁNGELES		Sesión en directo (2 hrs)				
3ª semana	Fase práctica: realización de retos en ATENEA / ELENA Sesión en directo (2 hrs)		Examen fase online				
4ª semana	Fase práctica: Realización de retos en ATENEA / ELENA		Sesión en directo (2 hrs)				

2º Módulo

Módulo Seguridad en correo electrónico

2º mes

30 horas de formación

Actualmente, el correo electrónico sigue siendo una de las herramientas más utilizadas por cualquier entorno corporativo para el intercambio de información. A pesar de que en los últimos años han surgido multitud de tecnologías y herramientas colaborativas para facilitar la comunicación y el intercambio de ficheros, el correo electrónico parece seguir siendo la herramienta predilecta de muchas empresas y usuarios. No es de extrañar, por tanto, que los atacantes traten de utilizar este medio para tratar de infectar y comprometer equipos.

Por ello, en este módulo se darán a conocer las técnicas más habituales de ingeniería social, así como los recursos utilizados por los atacantes para conseguir infectar un equipo u obtener información personal de un usuario. Asimismo, se ofrecerá un conjunto de pautas y recomendaciones para mitigar las acciones dañinas descritas.

El contenido del presente módulo será impartido durante cuatro (4) semanas de formación, divididas en una fase teórica y en una fase práctica.

A continuación se indica la programación y plazos para la realización de las diferentes actividades programadas para este módulo:

- Introducción al módulo mediante vídeo grabado por los expertos
- Fase teórica: realización de curso online
- Sesión de formación en directo a través de zoom
- Examen de evaluación
- Fase práctica: retos de ciberseguridad ATENEA / ELENA

2º mes

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
1ª semana	Fase teórica: Curso online seguridad en correo electrónico en ÁNGELES						
	Vídeo introductorio del módulo				Sesión en directo (2 hrs)		
2ª semana	Fase teórica: Curso online seguridad en correo electrónico en ÁNGELES						
			Sesión en directo (2 hrs)				
3ª semana	Fase practica: realización de retos en ATENEA / ELENA						
	Sesión en directo (2 hrs)		Examen fase online				
4ª semana	Fase práctica: Realización de retos en ATENEA / /ELENA						
			Sesión en directo (2 hrs)				

3er Módulo

Módulo Navegación segura

3er mes

30 horas de formación

En una época en la que cualquier usuario accede a su cuenta bancaria, realiza transacciones o compra todo tipo de productos a través de la web no es de extrañar que los ciberdelincuentes hayan focalizado sus ataques en el navegador web. Las múltiples vías de ataque que pueden llevarse a cabo para conseguir que el usuario ejecute código dañino, la facilidad para evadir medidas de seguridad tales como cortafuegos, IDS, etc., así como las posibilidades de post-explotación que ofrece el navegador hacen de éste un objetivo para los delincuentes.

Dado que actualmente el navegador web está expuesto a este tipo de peligros, el presente módulo tiene como objetivo, por un lado, concienciar al usuario sobre las técnicas más utilizadas por los cibercriminales y, por otro, ofrecer un conjunto de pautas para reducir la superficie de ataque de dichas acciones dañinas.

El contenido del presente módulo será impartido durante cuatro (4) semanas de formación, divididas en una fase teórica y en una fase práctica.

A continuación se indica la programación y plazos para la realización de las diferentes actividades programadas para este módulo:

- Introducción al módulo mediante vídeo grabado por los expertos
- Fase teórica: realización de curso online
- Sesión de formación en directo a través de zoom
- Examen de evaluación
- Fase práctica: retos de ciberseguridad ATENEA / ELENA

3º mes

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
1ª semana	Fase teórica: Curso online navegación segura en ÁNGELES						
	Vídeo introductorio del módulo				Sesión en directo (2 hrs)		
2ª semana	Fase teórica: Curso online navegación segura en ÁNGELES						
			Sesión en directo (2 hrs)				
3ª semana	Fase práctica: realización de retos en ATENEA / ELENA						
	Sesión en directo (2 hrs)		Examen fase online				
4ª semana	Fase práctica: realización de retos en ATENEA / ELENA						
			Sesión en directo (2 hrs)				

4º Módulo

Módulo Seguridad en dispositivos móviles

4º mes

30 horas de formación

En los últimos años, el desarrollo de los dispositivos y comunicaciones móviles junto con las tecnologías inalámbricas ha revolucionado la forma de trabajar y comunicarse. El uso creciente de estas tecnologías sitúa a los dispositivos móviles como uno de los objetivos principales para los atacantes.

Este módulo tiene como objetivo describir estas prácticas con el fin de ayudar a los usuarios finales a proteger y hacer un uso lo más seguro posible de los dispositivos móviles, profundizando en la configuración y utilización de los mecanismos de protección existentes en la actualidad. Para ello, se ofrecerá un conjunto de pautas y recomendaciones de seguridad para mitigar posibles acciones dañinas, dando a conocer las técnicas más habituales de ataque, así como los recursos utilizados por los atacantes para conseguir infectar un dispositivo móvil u obtener información personal de un usuario víctima.

El contenido del presente módulo será impartido durante cuatro (4) semanas de formación, divididas en una fase teórica y en una fase práctica.

A continuación se indica la programación y plazos para la realización de las diferentes actividades programadas para este módulo:

- Introducción al módulo mediante vídeo grabado por los expertos
- Fase teórica: realización de curso online
- Sesión de formación en directo a través de zoom
- Examen de evaluación
- Fase práctica: retos de ciberseguridad ATENEA / ELENA

4º mes

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
1ª semana	Fase teórica: Curso online seguridad en dispositivos móviles en ÁNGELES Vídeo introductorio del módulo				Sesión en directo (2 hrs)		
2ª semana	Fase teórica: Curso Online seguridad en dispositivos móviles en ÁNGELES		Sesión en directo (2 hrs)				
3ª semana	Fase práctica: realización de retos en ATENEA / ELENA Sesión en directo (2 hrs)		Examen fase online				
4ª semana	Fase práctica: realización de retos en ATENEA / ELENA		Sesión en directo (2 hrs)				

5º Módulo

Módulo Amenazas - Ransomware

5º mes

30 horas de formación

La familia de código dañino conocida como ransomware ha sido la amenaza más concurrente y dañina, con una gran evolución en los últimos años. Así, en un mundo en el que la mayoría de las fuentes relacionadas con la seguridad informática prevén que este tipo de amenazas siga aumentando, es importante saber cómo defenderse. Frente a los ataques informáticos es necesario actuar, al menos, en cuatro (4) fases distintas: prevención, detección, respuesta y remediación del ataque.

En este módulo se expondrán medidas aplicables a dichas fases, con el objetivo de prevenir este tipo de infecciones.

El contenido del presente módulo será impartido durante cuatro (4) semanas de formación, divididas en una fase teórica y en una fase práctica.

A continuación se indica la programación y plazos para la realización de las diferentes actividades programadas para este módulo:

Introducción al módulo mediante vídeo grabado por los expertos

Fase teórica: realización de curso online

Sesión de formación en directo a través de zoom

Examen de evaluación

Fase práctica: retos de ciberseguridad ATENEA / ELENA

5º mes

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
1ª semana	Fase teórica: Curso online Ciberamenazas – Ransomware en ÁNGELES						
	Vídeo introductorio del módulo				Sesión en directo (2 hrs)		
2ª semana	Fase teórica: Curso online Ciberamenazas – Ransomware en ÁNGELES						
			Sesión en directo (2 hrs)				
3ª semana	Fase práctica: realización de retos en ATENEA / ELENA						
	Sesión en directo (2 hrs)		Examen fase online				
4ª semana	Fase práctica: realización de retos en ATENEA / ELENA						
			Sesión en directo (2 hrs)				

6º Módulo

Módulo Gestión de Crisis

6º mes

30 horas de formación

Una cibercrisis es un acontecimiento del ámbito de la ciberseguridad con gran impacto sobre la actividad de la organización y que requiere tomar decisiones rápidas con información limitada. La probabilidad de ese acontecimiento dependerá del grado de preparación previa de la organización: será muy pequeña si se han tomado un gran número de medidas preventivas y progresivamente mayor cuanto menor sea el trabajo de prevención llevado a cabo con anterioridad.

Este módulo de gestión de ciberincidentes se basa en análisis detallados de episodios reales recientes de los que se derivan recomendaciones para abordar crisis en general, particularizando en cada caso la buena praxis para el gobierno de crisis derivadas de incidencias de ciberseguridad. En este módulo el alumno aprenderá qué es una cibercrisis, los procedimientos para gestionar situaciones de este tipo, y se darán a conocer casos de estudio y recomendaciones para manejar una crisis.

El contenido del presente módulo será impartido durante cuatro (4) semanas de formación, divididas en una fase teórica y en una fase práctica.

A continuación se indica la programación y plazos para la realización de las diferentes actividades programadas para este módulo:

- Introducción al módulo mediante vídeo grabado por los expertos
- Fase teórica: realización de curso online
- Sesión de formación en directo a través de zoom
- Examen de evaluación
- Fase práctica: retos de ciberseguridad ATENEA / ELENA

6º mes

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
1ª semana	Fase teórica: Curso online de gestión de cibercrisis en ÁNGELES						
	Vídeo introductorio del módulo				Sesión en directo (2 hrs)		
2ª semana	Fase teórica: Curso online de gestión de cibercrisis en ÁNGELES						
			Sesión en directo (2 hrs)				
3ª semana	Fase práctica: realización de retos en ATENEA / ELENA						
	Sesión en directo (2 hrs)		Examen fase online				
4ª semana	Fase práctica: realización de retos en ATENEA / ELENA						
			Sesión en directo (2 hrs)				