Guía de Seguridad de las TIC
CCN-STIC 891

Anexo V. Plan de Concienciación y Formación
Prestación sanitaria a pacientes
(Atención Primaria y Atención Especializada)

Febrero 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.02.08 12:34:20 +01'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

Fecha de Edición: febrero de 2024

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. OBJETO 4
2. ALCANCE 4
3. PLAN DE CONCIENCIACIÓN-FORMACIÓN 4
3.1 CURSO µCEENS 4
3.1.1 CONTENIDOS DE LOS MÓDULOS 5
3.2 CONCIENCIACIÓN 6
4. METODOLOGÍA 6
5. CICLO DE COBERTURA 7

1. OBJETO

El objeto del presente documento es establecer el Plan Concienciación-Formación que la Organización proporcionará para formar y concienciar al personal acerca de su papel y responsabilidad respecto a la seguridad de la propia Organización.

2. ALCANCE

Este Plan es de aplicación para todo el personal que, de manera permanente o eventual, preste sus servicios en la Organización dentro del ámbito de aplicación del proceso de Adecuación en el ENS.

En este sentido, se puede plantear con causa justificada un itinerario alternativo de acciones de Formación y Concienciación adaptado a las diferentes casuísticas que se pueden dar en las organizaciones como, por ejemplo: perfiles, tipología variada de personal, rotación del mismo, puesto de trabajo,… donde se podrán aplicar medidas compensatorias incorporando otro tipo de actividades formativas y de concienciación siempre y cuando se consigan alcanzar los objetivos marcados para lograr la certificación de conformidad en el ENS y así obtener un nivel de concienciación adecuado del personal en materia de ciberseguridad.

3. PLAN DE CONCIENCIACIÓN-FORMACIÓN

El Plan se basa en el Curso µCeENS, desarrollado a través de la Plataforma ÁNGELES en su apartado dedicado a cursos capacitación en el Esquema Nacional de Seguridad (https://angeles-elearning.ccn-cert.cni.es/course/view.php?id=204).

1. Todo el personal deber realizar el Curso µCeENS y aportar el certificado de su realización.
2. Desde la Plataforma de Gobernanza se ofrecerá la funcionalidad de realizar una formación personalizada, en su caso, donde las entidades podrán crear planes formativos que deseen para los diferentes perfiles.

3.1 CURSO µCeENS

A continuación, se indican los seis (6) módulos que conforman el Curso µCeENS con una duración de 75 horas, en modalidad asíncrona, que proporcionarán a los asistentes los elementos necesarios para conseguir la capacitación adecuada para el correcto empleo de las tecnologías e impulsar, al mismo tiempo, el conocimiento de las amenazas y vulnerabilidades asociadas a su uso.

1. Módulo de introducción a µCeENS.
2. Módulo de concienciación en ciberseguridad y ENS
3. Módulo básico de ciberseguridad
4. Módulo de seguridad en correo electrónico
5. Módulo de navegación segura
6. Módulo de seguridad en dispositivos móviles

3.1.1 Contenidos de los módulos

3.1.1.1 Módulo de introducción a µCeENS

La dificultad que encuentran organismos con pocos recursos para adecuarse al Esquema Nacional de seguridad ha hecho necesario definir un proceso que facilite la obtención de la Certificación.

µCeENS es el proceso completo para obtener la certificación de Conformidad en el ENS conforme a los requisitos determinados en un Perfil de Cumplimiento Específico, que se complementa con los servicios básicos de seguridad proporcionados por las herramientas del CCN en la modalidad ABS.

3.1.1.2 Módulo de concienciación en ciberseguridad y en el ENS

El objetivo es dar a conocer las principales amenazas que afectan al sector Público y mostrar como el ENS contribuye a mejorar la resiliencia y los mecanismos de defensa de las organizaciones.

3.1.1.3 Módulo básico de ciberseguridad

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.

3.1.1.4 Módulo de seguridad en correo electrónico

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 como vector de ataque.

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.

3.1.1.5 Módulo de navegación segura

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 la navegación web está expuesta 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.

3.1.1.6 Módulo de seguridad en dispositivos móviles

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.

3.2 CONCIENCIACIÓN

De la misma manera, semestralmente el Responsable de Seguridad se encargará de hacer llegar material divulgativo al personal objeto de este Plan para fortalecer y mejorar el conocimiento sobre aspectos clave de la seguridad de la información.

El material a distribuir se encuentra disponible en la Plataforma ÁNGELES, en su sección dedicada a “Formación 360”: https://angeles.ccn-cert.cni.es/es/formacion-360

4. METODOLOGÍA

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

Además, se proporciona a los alumnos material de estudio y apoyo necesario.

5. CICLO DE COBERTURA

Las actividades y actuaciones descritas en este plan de formación y concienciación deben ser llevadas a cabo durante un **periodo de dos (2) años**, hasta la siguiente auditoría de conformidad en el ENS.

Firmado:

Órgano competente

PUBLICACIONES DE DEFENSA
GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL