

USTIC-CONC 01/22. Programa “La ciberseguridad comienza por la concienciación”. Capítulo 1: ¿Y si esto fuera real?

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones **anuncia el inicio** de la publicación en este espacio **de un programa** de sensibilización y **concienciación en ciberseguridad**, dirigido a **todos los profesionales de la STIC**, bajo el título “**La ciberseguridad comienza por la concienciación**”.

Antecedentes

Concienciación y formación: Pilares de la gestión de la seguridad

La ciberseguridad se compone de tecnología, procesos y personas. Estos tres pilares son interdependientes. Es decir, las tecnologías no pueden proteger a las organizaciones si no se integran y utilizan correctamente o si los profesionales no conocen los procesos. Las medidas técnicas de seguridad deben funcionar en armonía con los procesos y las personas. Por ello, las personas son una pieza clave de la estrategia de ciberseguridad. En este contexto, **el desarrollo de una cultura de ciberseguridad es esencial para reducir los riesgos y ciberamenazas.**

Por tanto, **un elemento esencial para mejorar el nivel de seguridad en las organizaciones es la formación y concienciación de sus profesionales**, teniendo siempre presente el marco normativo y legal establecido y supervisando que se cumplen las buenas prácticas aprobadas. **Es necesario concienciar a todos los profesionales de la STIC en el uso de la seguridad y las implicaciones y riesgos de no asumirla. El objetivo es crear una cultura de ciberseguridad.**

Según la Agencia de Ciberseguridad de la Unión Europea (ENISA), la cultura de la seguridad se refiere a los conocimientos, hábitos, percepciones, actitudes, normas y valores de las personas en relación con la seguridad cibernética y la forma en que se manifiestan en el comportamiento de las personas con las tecnologías de la información.

Por tanto, apostar por la creación, desarrollo e integración de una cultura de ciberseguridad a través de la concienciación y formación es fundamental para gestionar la seguridad de la organización.

Para favorecer la implementación de una estrategia de concienciación, avanzando en la creación de una cultura de seguridad, la Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones cuenta con un servicio de formación y concienciación dentro de su cartera. Entre las actuaciones que se realizan, **se ha desarrollado el presente programa de concienciación para implicar a los profesionales TIC del SAS sobre el correcto uso de los sistemas de información y su papel como garantes de la información que manejan.** En el ámbito sanitario esto se hace imprescindible, debido a la sensibilidad de los datos que se tratan y almacenan en los sistemas de información.

Objetivos del Programa

El necesario equilibrio entre la usabilidad y la seguridad en el uso de la tecnología y el manejo de información provoca que mantener un adecuado nivel de ciberseguridad en las organizaciones requiera una adecuada implicación de las personas.

Los agentes de la amenaza son conscientes de esta realidad y sacan partido de ella utilizando a las personas como vector de entrada de sus ciberataques, haciendo uso de todo tipo de prácticas de ingeniería social: *phishing*, *smishing*, *vishing*, *media dropping*, etc. A esto hay que sumarle las brechas de ciberseguridad (por ejemplo, fugas de información) producidas por descuidos y prácticas inseguras de los empleados (mala praxis).

Esta situación provoca que se considere a las personas como un elemento crítico en su estrategia de protección, acuñando la famosa frase "las personas son el eslabón más débil de la cadena". No obstante, al igual que la conducta insegura de las personas introduce riesgos en la organización, una conducta segura puede convertirse en una salvaguarda muy efectiva: salvaguardas conductuales.

Por todo ello, resulta indiscutible la necesidad de trabajar en la dimensión de las personas, con el objetivo de **mejorar el nivel de ciberseguridad dentro de nuestra organización**, y así lo reflejan los principales marcos legales y normativos en materia de ciberseguridad tanto a nivel autonómico, nacional como internacional.

En este sentido, uno de los retos a los que desde la Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones se quiere dar respuesta es el de **incrementar el nivel de concienciación en seguridad de la información desde la prevención e involucrando a los profesionales de la STIC**.

Para ello, se hará llegar a todos los profesionales de la STIC aquellas nociones de seguridad, de manera que, se eviten riesgos procedentes de la falta de conocimientos sobre seguridad. Los objetivos que se persiguen son **fomentar una cultura de ciberseguridad en la organización, garantizar la integridad y confidencialidad de la información y aumentar la confianza en los sistemas de información**.

Para afrontar estos retos, resulta necesario el diseño e implantación de un plan de mejora del nivel de la cultura en ciberseguridad, que promueva los cambios en la conducta de los profesionales de la STIC mediante la realización de acciones de concienciación y formación en este ámbito.

Las acciones de concienciación tienen como objetivo **involucrar e implicar a las personas en la gestión de la ciberseguridad, ayudándoles a entender la importancia de su rol como parte activa de la estrategia de protección**.

Por su parte, las acciones formativas específicas permiten trasladar a las personas el conocimiento necesario para adoptar prácticas de comportamiento seguro que conduzcan a una gestión adecuada de los riesgos que les competen.

De esta forma, a las acciones formativas puestas en marcha este año dentro del Plan de Formación para Profesionales TIC 2022, como son las de Concienciación en Ciberseguridad para profesionales TIC, Análisis Forense Básico o Gestión de Seguridad de Proyectos TI, añadimos este programa mensual con acciones de sensibilización (concienciación) sobre ciberseguridad y que vienen a dar respuesta a los objetivos planteados.

Difusión del Programa

La difusión de este **programa bimensual** se realizará **a través de Confluence**. Bajo el título “La ciberseguridad comienza por la concienciación”, **se distribuirán en cada entrega diferentes tipos de material de sensibilización como pueden ser vídeos, infografías, documentos, consejos y buenas prácticas, recomendaciones, etc.**, destinados a fortalecer el conocimiento sobre aspectos clave de la seguridad de la información en todo el personal de la STIC. Algunos procederán de organizaciones referentes en ciberseguridad como ENISA, CCN-CERT, Andalucía-CERT o la ADA, por ejemplo y, otros, serán de elaboración propia.

La ejecución de este programa supone un avance en la generación de una cultura de seguridad con respecto al uso responsable de la información y de la necesidad de cambiar hábitos inseguros, mejorando la eficiencia de la gestión de seguridad de la información.

"La Ciberseguridad comienza por la concienciación". Semana Europea de la Ciberseguridad Sanitaria 2022. Capítulo 1: ¿Y si esto fuera real? Vídeo "Cyber Europe 2022 (Former CE2020)".

Este primer capítulo del programa "La ciberseguridad comienza por la concienciación" arranca con el siguiente vídeo que forma parte del material incluido en el ejercicio de ciberseguridad *Cyber Europe 2022* que la Agencia de Ciberseguridad de la Unión Europea (ENISA) organizó, con motivo de la Semana Europea de la Ciberseguridad Sanitaria 2022, estos pasados días 7 y 8 de junio para poner a prueba la respuesta a los ataques a las infraestructuras y servicios sanitarios de la UE y, que ha contado con la participación de 29 países de la UE y más de 800 expertos en ciberseguridad, entre los que se encuentra el equipo de la USTIC y de Andalucía-CERT.

El contenido del vídeo, titulado "*Cyber Europe 2022 (Former CE2020)*", muestra una situación que podría darse en el ámbito sanitario y que nos deja la siguiente pregunta final a modo de reflexión: "¿Y si esto fuera real?".

Podéis verlo aquí:

Your browser does not support the HTML5 video element

En caso de que no se reproduzca el anterior enlace , podéis hacerlo desde aquí: [Cyber Europe 2022 -former CE2020.mp4](#)

Para cualquier consulta o sugerencia respecto a este programa de concienciación, podéis contactar con [ustic.stic.sspa@juntadeandalucia.es](mailto:sspa@juntadeandalucia.es).

Gracias por vuestra atención y permaneced atentos al próximo capítulo... Saludos,

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud