



Entrevista con Ane Martínez Recio, facilitadora de los cursos 'Ciberseguridad; ¿me protegen? ¿nos protegemos? ¡me protejo!' y 'Ciberseguridad; si me toca proteger ¿dónde pongo el foco?'



Por tercer año consecutivo se insiste en la ciberseguridad como tema central dentro de la transformación digital que estamos viviendo como sociedad. ¿Por qué concederle un papel tan central?

Considero que es fundamental darse cuenta de que no basta con exigir y confiar en que las organizaciones para las que trabajamos o formamos parte protejan nuestros entornos tecnológicos de trabajo. La ciberseguridad es uno de los principales retos a los que, en esta era cada vez más digital, nos enfrentamos ciudadanía y organizaciones. **En un contexto de cada vez mayor virtualización en nuestras relaciones personales y profesionales, nuestra relación misma con la tecnología ha de cambiar.**

En la formación del año pasado, insistía en la importancia de incorporar en toda la formación tecnológica la **construcción y transmisión de una #Ciberética** en una sociedad cada vez más #Cibernética; reclamando ese papel activo y decisivo que tenemos como personas en toda interconectividad. Este año, quiero continuar haciendo hincapié en la **importancia de saberse parte fundamental, activa y decisiva de todo sistema de seguridad**. Asumir con responsabilidad la parte que nos toca a cada uno y cada una de nosotras dentro de la cadena de seguridad. Más si cabe si nos dedicamos a la formación y el acompañamiento de las personas más jóvenes, ya que **no sólo tenemos que asumir sino también transmitir**.

¿Por qué dos cursos diferenciados este año?

En la formación del año pasado nos dimos cuenta de que había **diferentes niveles de conocimiento y concienciación** y, sobre todo, diferentes ámbitos de aplicación de lo que íbamos a tratar. Por un lado, había personas usuarias y, por otro lado, estaban las personas técnicas responsables de implementar la seguridad en sus entornos.

Es por ello que, este año, afrontamos esos frentes con la oferta de dos cursos:

1.- **“Ciberseguridad; ¿me protegen?, ¿nos protegemos? ... ¡Me protejo!”;** curso orientado a personas usuarias sin responsabilidades de implementación de seguridad en entornos. En él aprenderemos a conocer y configurar nuestros dispositivos, a navegar de manera segura y, a conocer los diferentes tipos de ataques a los que estar en alerta y cómo reaccionar ante ellos.

2.- **“Ciberseguridad; si me toca proteger, ¿dónde pongo el foco?”;** curso más orientado a quienes tienen una responsabilidad más o menos técnica sobre los entornos tecnológicos. Para este curso el enfoque está más centrado en configuraciones básicas de múltiples dispositivos y redes (conociendo y optimizando routers y vpns). Pero, no sólo nos centraremos en ello, también afrontaremos la sensibilización y formación de las personas que componen esas redes de trabajo, ya que sabemos que somos origen y solución de los mayores incidentes de seguridad.

Según esto, la ciberseguridad trasciende a nivel global e individual, ¿podemos decir que es uno de los principales retos de esta década?

Desde el momento en el que cualquier persona puede ser objeto de un ciberataque, es vital conocer no sólo los beneficios, sino también los riesgos al usar tecnología. Riesgos unas veces basados en un no prestar atención a los protocolos de seguridad o, por desconocer los conceptos más básicos de la seguridad informática, otras por ataques externos o internos malintencionados y, por último, no podemos olvidar, los desastres naturales como cortes de electricidad, inundaciones e incendios que pueden provocar pérdida de información crucial para nosotros/as y nuestro entorno corporativo.

¿Por qué animarías a participar en los cursos?

Porque, según todo lo argumentado, el reto está en **interiorizar que las personas somos las responsables últimas** en la **identificación y protección de nuestros datos**. Y, considero que estos cursos pueden ser un buen inicio para ello.

Aprenderemos a identificar qué es lo que tenemos que proteger en cada caso, cuáles son los potenciales riesgos en cada caso y dispositivo y, sobre todo, a utilizar las medidas adecuadas para hacerles frente.