

CHARLA INFORMATIVA SEGURIDAD INFORMÁTICA

1 al 6 de Junio del 2019 impartido por Pilar Torres Lisa, Alberto Pérez Cizaurre

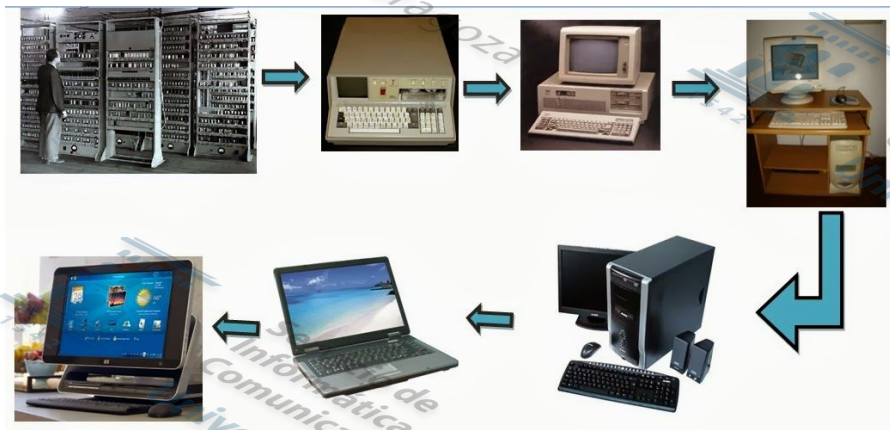


Universidad
Zaragoza

¿Por qué estamos aquí?



Contexto - Evolución de la Informática



“Nuevas situaciones”



Nuevas situaciones Nuevos Problemas



Paso de Físico A Virtual



BBVA

Buenos días :

Nos gustaria informarle que ha recibido un nuevo mensaje

Para consultar su buzón de correo, haga clic el siguiente enlace.

[Haga clic aqui](#) y iniciar sesion en su cuenta

Gracias por ser un cliente de BBVA

Tuyo sinceramente
Banco BBVA



Universidad
Zaragoza

Tipos de Delitos Informáticos más cometidos

Estafas

En primer lugar, las estafas. Es una de las formas delictivas más antiguas y comunes, que ha cobrado mayor vigor en la era de la informática. Las redes sociales junto a la globalización han permitido que los estafadores realicen con éxito su plan desde cualquier lugar del mundo.

Un factor que ha permitido su propagación es que pocas veces se denuncia esta transgresión y cuando lo hacen, generalmente, es después de haber modificado o eliminado las pruebas.

Acoso contra menores de edad

Plataformas como WhatsApp, Skype, redes sociales, foros privados y software de almacenamiento en la nube son las plataformas más usadas por los delincuentes para arremeter contra sus víctimas.

Cada año este tipo de delito supera los 500 casos, pero apenas el 10% llega a las instancias judiciales.

Falsificación de documentos

Este es un delito que, aunque oficialmente su porcentaje de ejecución es mínimo, está entre los más habituales. Consiste en la modificación de documentos laborales, personales, legales, imágenes y correos electrónicos.

Falsificación de identidad

La usurpación de identidad es otro delito informático bastante practicado. Por lo general, es una acción que va de la mano con una estafa. El correo electrónico y las redes sociales son los canales más susceptibles para poner en práctica este delito.

Cómo Puedo Evitarlo

Aplicar seguridad en la informática.

Formación Para poder aplicar medidas de seguridad.



¿Qué es la seguridad informática?

Podemos definir qué es la seguridad informática como el proceso de prevenir y detectar el uso no autorizado de un sistema informático.

Las cuatro áreas principales que cubre la seguridad informática

Confidencialidad

Integridad

Disponibilidad

Autenticidad

CONFIDENCIALIDAD

Confidencialidad: Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.

La información en muchas ocasiones tiene valor mientras siga siendo confidencial.

Muchas veces la información debe ser confidencial derivada de leyes.

INTEGRIDAD

Integridad: Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.

¿De qué nos serviría nuestra información si hemos conseguido mantenerla confidencial pero se ha alterado sin que nosotros queramos?

DISPONIBILIDAD

Disponibilidad: Los datos deben estar disponibles para los usuarios cuando sea necesario.

AUTENTICACIÓN

Autenticación: Estás realmente comunicándote con los que piensas que te estás comunicando.



Problemas para nosotros y para la UNIVERSIDAD DE ZARAGOZA

SI NO APLICAS MEDIDAS TENDREMOS
PROBLEMAS Y CONSECUENCIAS PENALES /
DISCIPLINARIAS / DINERARIAS.....



La importancia de la formación

El curso se realizará online dentro del ADD:

<https://moodle2.unizar.es/add/course/view.php?id=21388>

Cada uno puede empezar cuando quiera.

No hay un tiempo en el que terminarlo.

Nivel Elemental:

La información

Los soportes

El puesto de trabajo

Los dispositivos móviles.

