

RECUERDA: KIT DE CONCIENCIACIÓN EL PUESTO DE TRABAJO

- ! Tu puesto de trabajo es clave para la **seguridad de la información**.
- ! **Guarda** tu información en un lugar adecuado.
- ! **Utiliza mobiliario** con cierres, cajas fuertes o armarios ignífugos.
- ! **Destruye** la documentación de forma segura.
- ! **Utiliza contraseñas seguras**.
- ! **Tus contraseñas deben ser secretas**.
- ! **Usa métodos de autenticación** combinados para mayor seguridad.
- ! **Implanta** una política de mesas limpias y comprueba que se aplica periódicamente.
- ! **Aprende** a detectar los ataques de ingeniería social y cómo defenderte.
- ! **Sé precavido** cuando uses el correo y las redes sociales, para evitar fugas de información.



CONTÁCTANOS



Producto diseñado y desarrollado por INCIBE.
Adaptación a universidades realizada por MetaRed.

INSTITUTO NACIONAL DE
CIBERSEGURIDAD
SPANISH NATIONAL
CYBERSECURITY INSTITUTE

 **incibe_**
www.incibe.es

Kit de Concienciación EL PUESTO DE TRABAJO



 **crue**
Universidades
Españolas

El puesto de trabajo es un **PUNTO CLAVE** desde el punto de vista de la **SEGURIDAD DE LA INFORMACIÓN**.



Debemos implantar **LAS MEDIDAS DE SEGURIDAD** oportunas para la protección de la información tanto en soporte papel como en formato electrónico.

Es recomendable guardar nuestra información en una **UBICACIÓN ADECUADA** fuera del alcance de posibles riesgos, como fugas de agua.



Es necesario emplear **MOBILIARIO** que **CONTRIBUYA A LA PROTECCIÓN** de la información confidencial, como armarios con dispositivos de cierre, cajas fuertes o armarios ignífugos.



Es necesario aplicar un proceso de **DESTRUCCIÓN SEGURA** a la hora de eliminar la documentación, así como establecer los **ACUERDOS DE CONFIDENCIALIDAD** pertinentes si se delega su destrucción.



Es necesario implantar una **POLÍTICA DE CONTRASEÑAS SEGURAS** en nuestra organización.

Es fundamental que **LAS CONTRASEÑAS SEAN SECRETAS**, no debemos anotarlas ni compartirlas.



Un **MÉTODO DE AUTENTICACIÓN** es aquella técnica o procedimiento que permite verificar que un usuario es quien dice ser.

Existen métodos de autenticación **DIFERENTES**, como por ejemplo, el uso de una contraseña, de una tarjeta de acceso o de la huella digital. Pero para mayor seguridad se utiliza más de uno, lo que se conoce como **MÉTODOS COMBINADOS**.



Es necesario implantar una **POLÍTICA DE MESAS LIMPIAS**, junto a un procedimiento de auditoría periódica que lo valide.



LA INGENIERÍA SOCIAL tiene como objetivo a los empleados de nuestra organización y permite obtener información confidencial de las víctimas y su organización.



Es fundamental **FORMARSE Y CONCIENCIARSE** en materia de seguridad de la información.



La mayoría **DE LAS FUGAS DE INFORMACIÓN** se producen en el puesto de trabajo. Pueden ser ocasionadas por un fallo, un error o actos malintencionados.

Es recomendable ser cuidadoso con el uso del correo y las redes sociales, para evitar posibles fugas de información.