



Recomendaciones en Ciberseguridad

La amenaza más seria para un sistema de información son las personas. Por esta razón, la formación y sensibilización del personal son la mejor defensa para prevenir y detectar contratiempos. Es muy importante definir, documentar y difundir una política de seguridad que demuestre el compromiso de la organización con la seguridad, así como desarrollar normativas que recojan las obligaciones a las que están sujetos los usuarios.

COPIAS DE SEGURIDAD



Realiza copias de seguridad periódicas

BORRADO



Haz un borrado seguro de la información una vez que esta ya no sea necesaria.

ENLACES Y DESCARGAS



No abras ningún enlace ni fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.

ACTUALIZACIONES



Mantén actualizadas las aplicaciones y el sistema operativo.



CIBERSEGURIDAD

La cultura de la ciberseguridad y la concienciación del empleado deben ser objetivos prioritarios para las organizaciones.

CIFRADO



Cifra la información sensible, no hay otra alternativa.

CONTRASEÑAS



Utiliza contraseñas adaptadas a la funcionalidad y utiliza la doble autenticación.

PRECAUCIÓN



Limita la superficie de exposición a las amenazas

SOFTWARE DE SEGURIDAD



Utiliza software de seguridad, herramientas antivirus y antimalware, cortafuegos personales, herramientas de borrado seguro, etc.



centro criptológico nacional