- CONTRASENAS
- ADMINISTRACIÓN DE CONTRASEÑAS
- REDUCIR ACCESO A CONTENIDOS Y DATOS
- PROTEGER DISPOSITIVOS
- DESACTIVAR LA GEOLOCALIZACIÓN
- CUIDADOS EN LA PUBLICACIÓN DE CONTENIDOS
- SERVICIOS DE COMUNICACION SEGUROS
- CONFIGURAR LOS CONTROLES DE PRIVACIDAD EN REDES
- BORRAR REGISTRO DE LLAMADAS
- VERIFICACIÓN EN 2 PASOS
- NAVEGADOR
- BUSCADOR
- RECOMENDACIONES PARA EVITAR ENGAÑOS QUE BUSCAN OBTENER INFORMACIÓN PERSONAL SENSIBLE DE FORMA FRAUDULENTA

TIPS DE SEGURIDAD DIGITAL

Datysoc INDELA

CONTRASEÑAS

- sin información personal
- largas (de 8 0 +caracteres)
- contienen mayúsculas, minúsculas, símbolos y números privada, no la compartes con nadie
- única, no usar la misma contraseña en varias plataformas o servicios
- importante cambiarlas con periodicidad y cerrar sesiones.

https://www.security.org/how-secure-is-my-password/

ADMINISTRACIÓN DE CONTRASEÑAS

- KeePass es un administrador de contraseñas gratuito de código abierto https://keepass.info/
- Dashlane es una aplicación móvil y web que simplifica la administración de contraseñas.Tiene una membresía gratuita hasta de 20 contraseñas. https://support.dashlane.com/hc/es/articles/4679936285458--Qu%C3%A9-es-Dashlane#:~:text=Dashlane%20es%20una%20aplicaci%C3%B3n%20m%C3%B3vil,sociales%2C%20de%20compras%20y%20bancaria.
- Lastpass es un gestor de contraseñas pago https://www.lastpass.com/es/why-lastpass

REDUCIR ACCESO A CONTENIDOS Y DATOS

- Página web o servicio en línea con información: chequear que sea una conexión encriptada (el enlace tiene que empezar con https://)
- Instalar en Firefox, Chrome y Safari, extensiones que mejoran tu privacidad: Privacy Badger que bloquea rastreadores espías, uBlock Origin, AdBlock que bloquean publicidad.

PROTEGER DISPOSITIVOS

- Bloquear el teléfono y/o dispositivos con una contraseña, código o patrón
- Hacer copias de seguridad de la info y guardarla en lugares seguros
- Cifrar tus archivos, el contenido de tu disco duro y el celular.

DESACTIVAR LA GEOLOCALIZACIÓN

Activar y desactivar la geolocalización en las aplicaciones y usarla en ocasiones que sea necesaria.

CUIDADOS EN LA PUBLICACIÓN DE CONTENIDOS

- Usar perfiles privados a los que solo acceden los contactos seleccionados.
- Antes de publicar imágenes y /o contenidos de eventos públicos analizar si la información acerca de personas, lugares u otras pueden ser riesgoso para alguna de las personas implicadas.
- Contar con el consentimiento para publicar sobre personas y eventos.
- establecer acuerdos acerca de qué y cómo publicar información con todas las personas presentes en un evento público.
- Difuminar, oscurecer o volver borrosas las caras en tus fotografías antes de publicar
- Ej. app ObscuraCam https://guardianproject.info/apps/obscuracam

SERVICIOS DE COMUNICACION SEGUROS

Signal: servicio de mensajería cifrado que permite mensajes de texto y llamadas de voz con cifrado de extremo a extremo.
https://signal.org/es/

CONFIGURAR LOS CONTROLES DE PRIVACIDAD EN REDES

- En Facebook: Visita Configuración > «Privacidad» y asegúrate de que estás de acuerdo con todas las opciones. Te recomendamos la opción «Comprobación rápida de privacidad» en el menú de Ayuda.
  Además, en la sección de Privacidad, puedes decidir:
  i) quién puede ver tus contenidos
  ii) quién puede ponerse en contacto contigo
  iii) quién puede buscarte.
- En Instagram: Revisa las opciones en Configuración «Privacidad» y «Seguridad» para configurar tu cuenta como privada y decidir quiénes pueden enviarte mensajes.
- En X(Ex-Twitter: Ve a la sección de configuración y privacidad.
- En TikTok: Pulsa Privacidad > Ajustes > Configuración de privacidad y activa la opción ‘Cuenta privada’. Allí, tendrás la posibilidad de elegir quién podrá enviarte mensajes, ver tus vídeos, comentar tus publicaciones.

BORRAR REGISTRO DE LLAMADAS

Borrar el historial de llamadas y mensajes que no son necesarios.

VERIFICACIÓN EN 2 PASOS

Agrega una capa de seguridad a las cuentas de redes sociales, correo electrónico y mensajería instantánea. Disponible en: Gmail, Hotmail, Yahoo, Facebook, Twitter y Whatsapp.

Si quieres activar la verificación de dos pasos sigue estos pasos (cambian para cada servicio):

- Ir a configuración de tu servicio
- Buscar la opción de seguridad o privacidad
- Encontrar la opción activar verificación de dos pasos.
- Puede solicitar un número telefónico para la activación.
- Por ultimo escanea el código QR para activar un número aleatorio de seis dígitos.

NAVEGADOR

Tor es un navegador que protege del rastreo, la vigilancia y la censura.
https://www.torproject.org/es/download/

Firefox es un navegador gratuito mozilla
https://www.mozilla.org/en-US/firefox/new/

Brave es un navegador bastante nuevo pero con buenas características
https://brave.com/

BUSCADOR

DuckDuckGo es un buscador privado y gratuito
https://duckduckgo.com/

Startpage es un buscador sin historial de búsquedas, sin publicidad dirigida y sin huella digital
https://www.startpage.com/es/

MetaGer es un buscador sin anuncios y que ofrece anonimización en las búsquedas
https://metager.de/es-ES

RECOMENDACIONES PARA EVITAR ENGAÑOS QUE BUSCAN OBTENER INFORMACIÓN PERSONAL SENSIBLE DE FORMA FRAUDULENTA

- No descargar archivos de dudosa procedencia
- No dar clic en enlaces sospechosos
- Actualizar el sistema operativo de los equipos
- Usar un antivirus actualizado en los dispositivos
- Ante un comportamiento extraño buscar asesoría.
- No dar contraseñas por msjs, por servicios de mensajería, ni por llamadas.
- Para Windows descargar Spybot que permite eliminar cierto tipo de malware (programa malicioso), spyware (espía) y adware (publicidad).