

Canoa salvavidas

para navegar por internet



Entre menos información personal compartas en redes sociales, más seguro o segura estás.

Protege tu identidad en redes sociales: Evita compartir información personal sensible en tus perfiles de redes sociales, como tu dirección, número de teléfono o detalles sobre tu trabajo y tu familia. Mantén esos datos privados y limita la cantidad de información visible en tus perfiles públicos.



Las mejores aplicaciones de mensajería son las que cifran tus chats de extremo a extremo.

Con ellas solo tú y con quién hablas pueden acceder a la conversación. Recomendamos usar Signal y WhatsApp. Evita compartir información confidencial en plataformas que no cifren los mensajes, como Telegram en su configuración predeterminada. Ñapa: No olvides activar la verificación en dos pasos.



¡Cuidado! En las aguas digitales también hay virus y robos

Para prevenir caer en phishing (robo de información) o en malwares (virus) no des clic en enlaces de fuentes desconocidas o sospechosas, tampoco descargues archivos de esos lugares. Aprende a reconocer señales de phishing, en correos electrónicos o mensajes de texto que piden tu información personal o contraseñas.



Doble nudo para nuestras cuentas

Fortalece su seguridad utilizando contraseñas seguras, estas deben ser largas, complejas y únicas para cada uno de tus correos electrónicos y cuentas en redes sociales. Activa la autenticación de dos factores - 2FA - (el mensaje de texto que te llega con un código único para ingresar) para agregar una capa adicional de seguridad a tus cuentas. Para no perder las contraseñas, usa un gestor de contraseñas como KeePassXC o Bitwarden.



Cuida la información que compartes en línea.

Antes de publicar contenido en redes sociales, evalúa el impacto potencial que podría tener en tu seguridad o en la de otras personas. Ten cuidado con las etiquetas en fotos o vídeos. Evita publicar información confidencial o comprometedor sobre ti o tu organización, por ejemplo temas de reunión o lugares de encuentro. Para la difusión de información se pueden utilizar boletines cifrados o plataformas seguras para la compartición de documentos, esto evita tener que publicar información crítica directamente en redes sociales.



La privacidad ha salido del grupo

Sé consciente de los riesgos en grupos de WhatsApp y Telegram: Controla la configuración de privacidad de tus grupos ¿Sabes quienes son todas las personas que están en el grupo? Evita compartir información sensible en grupos donde no todas las personas participantes son de confianza. Ñapa: Mantén un grupo más pequeño y controlado para compartir información estratégica y sensible.



Tú puedes ayudar a hacer de internet un lugar seguro

Bloquea y denuncia comportamientos abusivos o amenazantes en plataformas digitales (usa las opciones de reportar en Facebook, Instagram y WhatsApp). Mantén registros (pantallazos, números de teléfono, perfiles en redes, enlaces de sitios web) de cualquier incidente de acoso y denúncialo a las autoridades competentes. En <https://acoso.online> encontrarás recursos que pueden ayudarte cuando se presente un incidente. acoso.online



Ponle un chaleco salvavidas a tus datos respaldando la información

Realiza copias de seguridad periódicas de la información importante almacenada en tu celular, computador, etc y en la nube. Mantén los datos respaldados en lugares seguros (disco duro externo cifrado, usb cifrada) y fuera del alcance de personas no autorizadas. Para copias de seguridad cifradas puedes utilizar Veracrypt.



Mi primer territorio soy yo, me cuido y cuido el medio ambiente

Prioriza el autocuidado y busca apoyo emocional. Mejorar tu seguridad digital impacta de forma positiva en tu bienestar. Establecer alianzas y colaboraciones con otras personas y organizaciones puede ser una buena idea.



Compartir información como una muestra de cariño

Comparte conocimientos y mejores prácticas en seguridad digital para fortalecer la seguridad colectiva. Promueve la importancia de proteger la privacidad y la información sensible en línea.



<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD

Fundación
Karisma

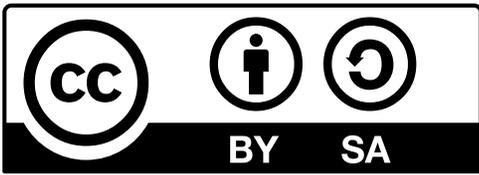


para navegar por internet

Canoa salvavidas

Este material circula bajo una licencia Creative Commons CC BY-SA 4.0.

Eres libre de:
Compartir — copiar y redistribuir el material en cualquier medio o formato
Adaptar — remezclar, transformar y construir a partir del material para cualquier propósito, incluso comercialmente.



Así como en el mar o en el río, navegar por internet tiene sus peligros; eso no quiere decir que vas a dejar de hacerlo, sino que puedes mejorar tus prácticas de autocuidado y seguridad digital para disfrutar de la navegación. Por eso les compartimos esta canoa salvavidas con tips para proteger tu privacidad, identidad e información.

Guía de seguridad digital para defensores y defensoras del medio ambiente.



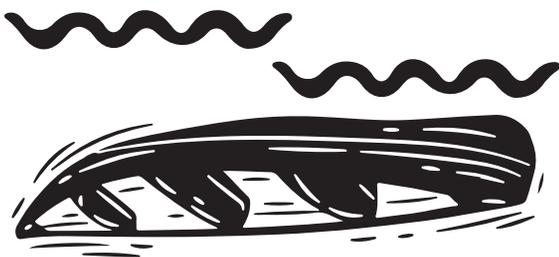
Canoa salvavidas

para navegar por internet



<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD

Fundación Karisma



Desde Karisma queremos compartir unas recomendaciones para que quienes defienden el medio ambiente en Colombia continúen con la importante tarea de proteger nuestro planeta, protegiendo su seguridad en línea.

