Nicaragua Cibersegura

Defensores del Cifrado.

CIFRADO DE EXTREMO A EXTREMO

Aplicaciones de mensajería segura

El cifrado de extremo a extremo es el acto de aplicar un cifrado a los mensajes de un dispositivo de forma que solo el dispositivo al que se le envía pueda descifrarlo. El mensaje viaja desde el remitente al destinatario en forma cifrada.

TELEGRAM

Tiene dos capas de cifrado seguro. El cifrado servidor-cliente es usado en los Chats en la Nube (privados y grupales). Los chats secretos usan una capa adicional de cifrado cliente-cliente. Todos los datos, sin importar su tipo, son cifrados de la misma manera, ya sean textos, multimedia o archivos.

WHATSAPP

El cifrado de extremo a extremo garantiza que solo tú y la persona con quien te comuniques puedan leer o escuchar lo que se envía, y que nadie más, ni siquiera WhatsApp, pueda hacerlo. Esto ocurre debido a que, gracias al cifrado de extremo a extremo, los mensajes se aseguran con un candado y solo tú y el destinatario tienen la llave especial que se necesita para desbloquearlos y leerlos. Todo esto se lleva a cabo de manera automática, sin necesidad de activar ninguna configuración especial para proteger tus mensajes.

SIGNAL

Utiliza un protocolo de cifrado de extremo a extremo llamado Open Whispers Systems para todas las comunicaciones, lo que quiere decir que los mensajes salen de tu móvil ya cifrados, y sólo se descifran cuando llegan al móvil del receptor. De esta manera, si alguien los intercepta por el camino, no podrá leerlos. El cifrado de Signal es tan popular que la propia WhatsApp decidió utilizarlo cuando implementó este tipo de tecnología.

THREEMA

Contiene un paquete de medidas muy sólido para asegurar la privacidad del usuario. De esta manera, utiliza el protocolo de criptografía NaCi para cifrar la biblioteca de archivos, y no es necesario registrarse con un número de teléfono,
ya que la app asigna a cada usuario una dirección ID o una contraseña de 8 dígitos para entrar en la app y que se genere un perfil, pero no aparece ni el número ni ningún dato personal.

TIPOS DE CIFRADO

1

Cifrado Asimétrico

Es aquel que utiliza la misma clave para cifrar y descifrar el mensaje y que previamente deben conocer el emisor y el receptor

2

Cifrado Simétrico

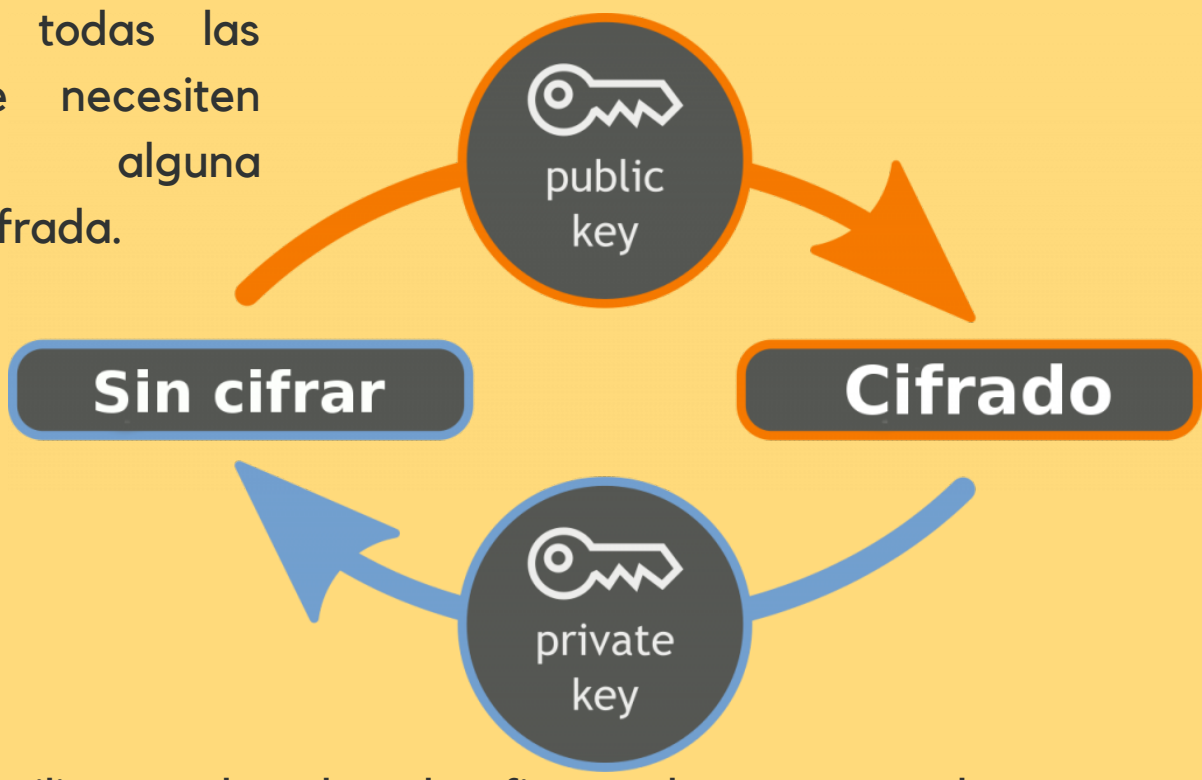
Es aquel que utiliza dos claves. La pública y la privada.

Clave Pública

La pública es aquella que se puede difundir sin problemas, a todas las personas que necesiten mandarle alguna información cifrada.

Clave Privada

La privada es aquella que no se debe revelar nunca.



También se utiliza mucho el poder firmar documentos, de esta forma se certifica al emisor, firmando con la clave privada y verificando la identidad del receptor con la clave pública.

Ventajas y Desventajas de un método u otro

Velocidad: el cifrado simétrico es mucha más rápido y ágil. El cifrado asimétrico es mucho más lento.

Seguridad: el cifrado simétrico no es tan seguro, ya que el hecho de publicar la clave lo hace muy vulnerable. El cifrado asimétrico tiene como ventaja, el hecho de que puede comunicar en forma segura, claves públicas a terceros. Este cifrado entrega la clave pública manteniendo a clave privada el usuario.

Número de claves: la administración de claves también es un beneficio al usar el cifrado asimétrico, se necesita sólo un par de claves por usuario, para cada uno, para poder cifrar mensajes para todos los demás usuarios. En cambio, con el cifrado simétrico, a medida que aumenta el número de usuarios, aumenta el número de claves.

www.nicaraguacibersegura.org
@defensoresdelcifrado
@nicaraguacibersegura
@nic_cibersegura

Nicaragua Cibersegura
Defensores del Cifrado.

WHATSAPP VS TELEGRAM VS SIGNAL

¿CUÁL ES LA APP DE MENSAJERÍA MÁS SEGURA?

Permisos

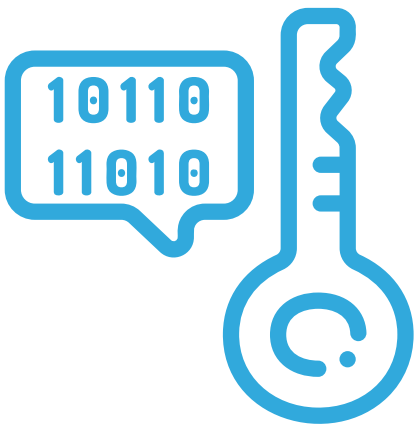
Si la privacidad es nuestra prioridad, lo primero que tenemos que tener en cuenta a la hora de instalar una aplicación son los permisos que estas requieren. Los permisos solo se piden si son necesarios, y eres libre de no otorgarlos si no quieres usar esa función.

WhatsApp y Telegram necesitan obligatoriamente el acceso a tus contactos, y te los pedirán constantemente si se lo niegas. En Signal, sin embargo, es opcional pues puedes iniciar una conversación escribiendo el número de teléfono manualmente.

Protección de acceso (PIN, huella)

¿Si una persona tiene acceso a tu teléfono, puede leer tus chats de Telegram, WhatsApp y Signal? Sin tener en cuenta aplicaciones de terceros o funciones añadidas de capas Android, solo Telegram y Signal te permiten proteger tus chats, aunque no esté activada de forma predeterminada. WhatsApp no incluye ninguna protección.

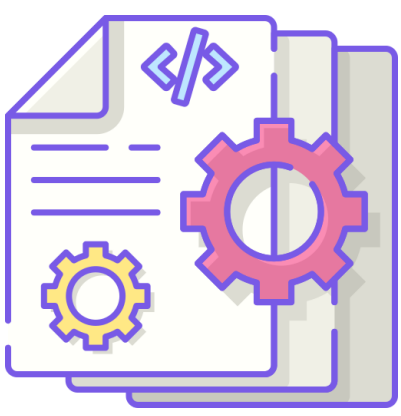
Telegram te da algo más de control sobre esta protección, permitiéndote proteger tus chats bien mediante un código PIN o mediante una contraseña y pudiendo bloquear el acceso en cualquier momento tocando en el icono del candado. En Signal el bloqueo es compartido con el de Android y el bloqueo es automático tras un periodo de tiempo.



Cifrado

Mientras que WhatsApp y Signal usan el cifrado de extremo a extremo para todas las comunicaciones, en Telegram solo se usa en los chats secretos, que añaden otras funciones extra de seguridad como protección contra capturas de pantalla y mensajes que se autodestruyen.

Sin chats secretos Telegram sigue cifrando los mensajes entre el cliente y la nube y solo se tiene constancia de una vulnerabilidad en la implementación, que data de 2013.



Metadatos

Con el cifrado nadie puede leer tus mensajes, pero sí saber con quién hablas y desde dónde, por los metadatos.

Asegurar que tus mensajes se transmiten de forma segura y sin que nadie los pueda interceptar es importante, pero tan importante es el contenido del mensaje como sus metadatos. En este contexto se refiere a toda la información adicional que acompaña a un mensaje, sin incluir su propio contenido.

WhatsApp recopila una buena cantidad de metadatos de sus usuarios como direcciones IP, fechas de uso, teléfono y modelo, operador de red, número de teléfono, identificador único de dispositivo, ubicación y contactos. Cruzando esta información, incluso sin poder leer el contenido de los mensajes, se pueden hacer suposiciones bastante aproximadas sobre con quién hablas y en algunos casos de qué.

Telegram está basado en la nube así que técnicamente todos tus mensajes, fotos y archivos enviados en conversaciones no privadas están almacenados (cifrados, eso sí) en sus servidores.

Signal es la única aplicación entre esta comparativa que reduce al mínimo los metadatos que guarda. Solo archiva la última vez que te conectaste (el día, ni siquiera la hora) y el número de teléfono de tu cuenta.

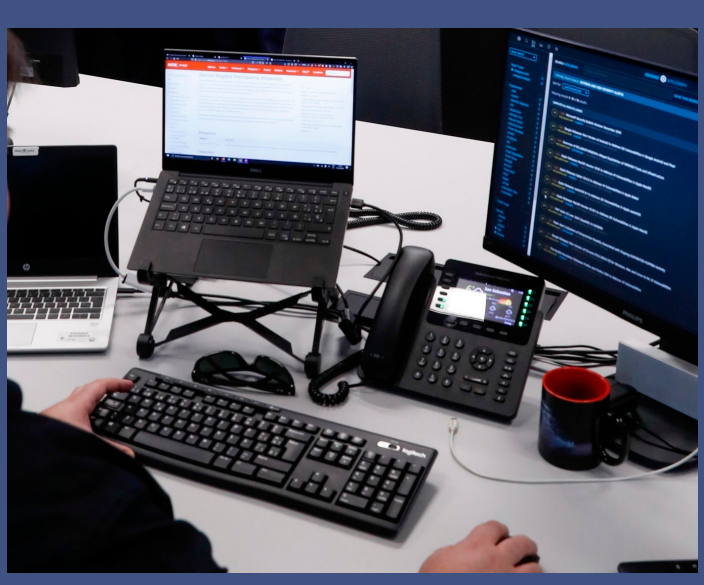
LEY ESPECIAL DE CIBERDELITOS EN NICARAGUA

Se castigara con cárcel las "noticias falsas" en medios de comunicación y redes sociales.

La cuestionada iniciativa fue aprobada el 27 de octubre de 2020 con 70 votos a favor, todos de diputados del partido gobernante.

FACULTADES DE LA LEY

Autoriza al Ministerio de Gobernación, la policía y a la estatal Empresa Nicaragüense de Telecomunicaciones (TELCOR) a investigar y perseguir los delitos que sean cometidos por medios de comunicación y aplicaciones informáticas que producen, reproducen y transmiten gráficos y textos.



Los jueces podrán autorizar a la policía intervenir y acceder al sistema informático de los sospechosos y ordenar a los proveedores del servicio de internet grabar y facilitar datos del usuario que es investigado.

www.nicaraguacibersegura.org

@defensoresdelcifrado

@nicaraguacibersegura

@nic_cibersegura

Nicaragua Cibersegura

Defensores del Cifrado.

¿Sabes cuanto valen tus datos en la Deep Web?

Las cifras dependeran de la importancia del documento y país de origen.

Licencias de conducir

Entre $6 y $20 dólares

Datos de tarjeta de crédito

Entre $6 y $10 dólares

Pasaportes escaneados

Entre $6 y $15 dólares

Servicios de Suscripción

Entre $1 a $7 dólares

Documento de identidad

Entre $1 a $8 dólares

Selfie con documentos (Pasaporte, Licencia de conducir)

Entre $1 a $8 dólares

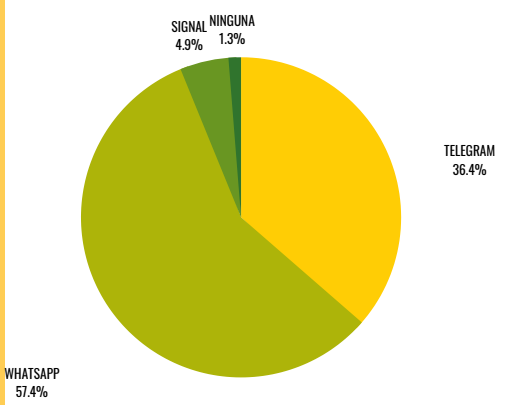
Nicaragua Cibersegura

Defensores del Cifrado.

www.nicaraguacibersegura.org

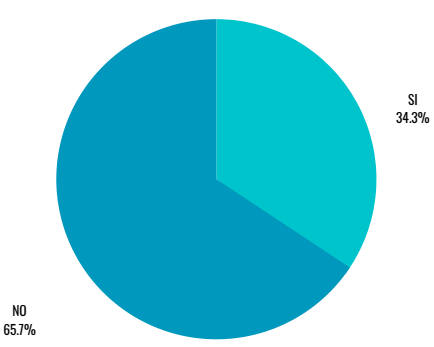
¿CONOCEN LOS JOVENES SOBRE CIFRADO DE DATOS Y GESTIÓN DE PRIVACIDAD EN NICARAGUA?

En una encuesta online realizada a universitarios entre las edadades de 18 a 35 años se determina que:



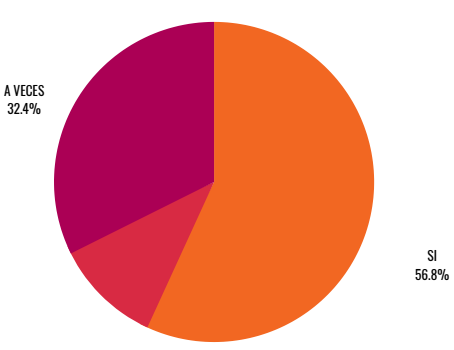
EL 91.2% UTILIZA WHATSAPP DE PREFERENCIA COMO APP DE MENSAJERIA SEGURA.

Mientras tanto el 57.8% ya comienza a utilizar Telegram. Frente a un escaso 7.8% representado por usuarios de Signal.



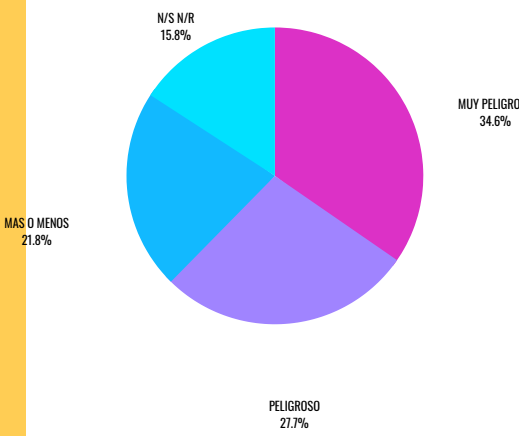
EL 65.7% DE LOS ENCUESTADOS NO SABE O NO CONOCE SOBRE EL CIFRADO DE DATOS.

Unicamente el 34.3% manifiesta conocerlo.



EL 56.9% ADUCE QUE LE PREOCUPA SU PRIVACIDAD ONLINE.

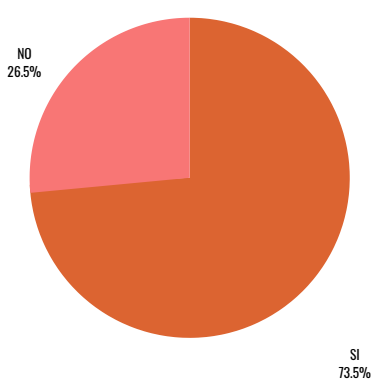
El 32.4% a veces siente un poco de temor, en cambio el 10.8% no siente que su privacidad este en peligro.



EL 34.3% Y EL 27.5% DE LOS ENCUESTADOS CONSIDERA QUE ES UN RIESGO COMPARTIR INFORMACIÓN PRIVADA A TRAVÉS DE INTERNET.

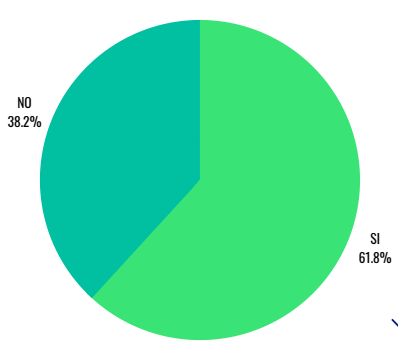
Un 21.6% considera que es más o menos seguro por los mecanismos que brindan las distintas plataformas digitales.

El 15.7% desconoce qué tan seguro sea.



EL 73.5% EXPRESA QUE CONFIGURAR LA PRIVACIDAD EN LAS REDES SOCIALES NO GARANTIZA UNA PRIVACIDAD TOTAL YA QUE DEPENDERÁ DE QUE PUBLICAMOS Y QUIENES TIENEN ACCESO A VER LA PUBLICACIÓN.

El 26.5% se muestra confiado al definir su perfil como privado.



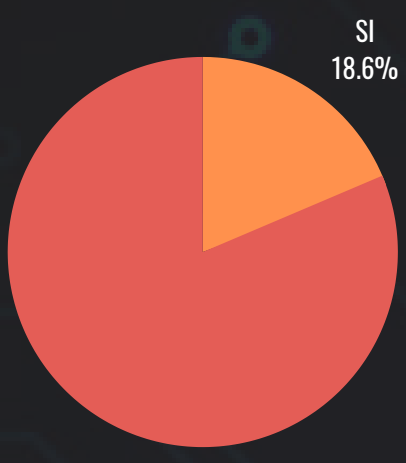
UN 61.8% REFIERE QUE UTILIZA DE FORMA RESPONSABLE EL INTERNET, FRENTE A UN 38.2% QUE CONSIDERA NO HACERLO.

Nicaragua Cibersegura

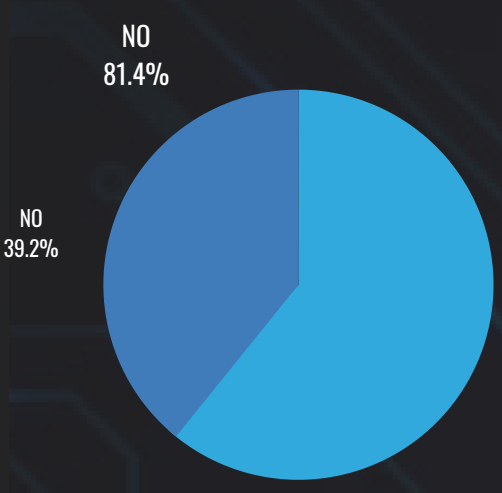
Defensores del Cifrado.

MÁS INFORMACIÓN EN WWW.NICARAGUACIBERSEGURA.ORG

LEYES RELACIONADAS AL USO DE INTERNET EN NICARAGUA

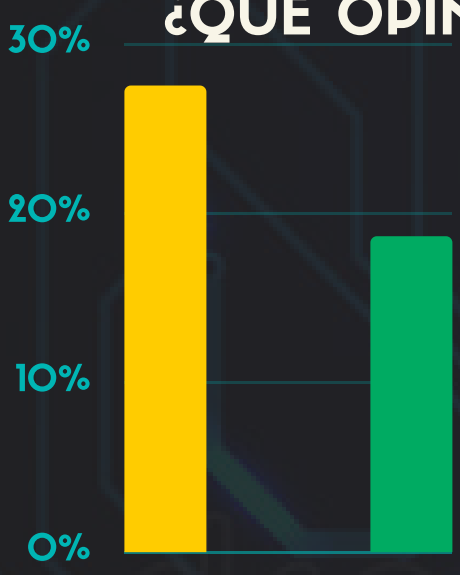


RESULTA RELEVANTE QUE EL 81.4% DE LOS ENCUESTADOS, DESCONOZCAN DE LA EXISTENCIA DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES, FRENTE A UN ESCASO 18.6%, QUE SI RECONOCE SABER DE SU EXISTENCIA PERO QUE NO SE ASEGURAN SEA IMPLEMENTADA.



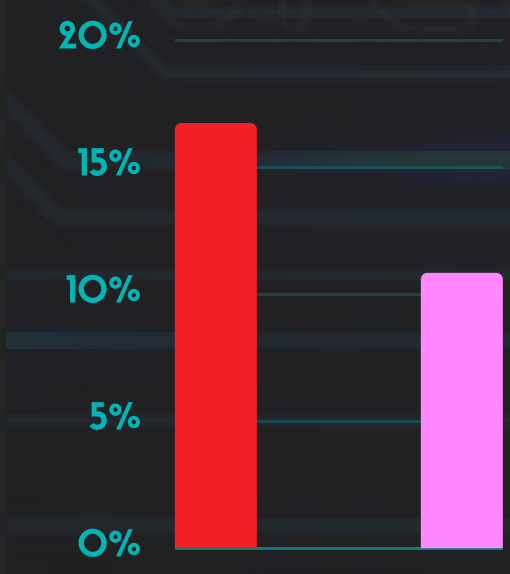
AL CONSULTAR SOBRE LA APROBACIÓN DE LA LEY 1042, LEY ESPECIAL DE CIBERDELITOS, LA GRAN MAYORÍA QUE REPRESENTA EL 60.8% CONOCE DE ESTA LEY, MIENTRAS QUE UN 39.2% DESCONOCE DE SU EXISTENCIA.

¿QUE OPINA DE LA LEY DE CIBERDELITOS?



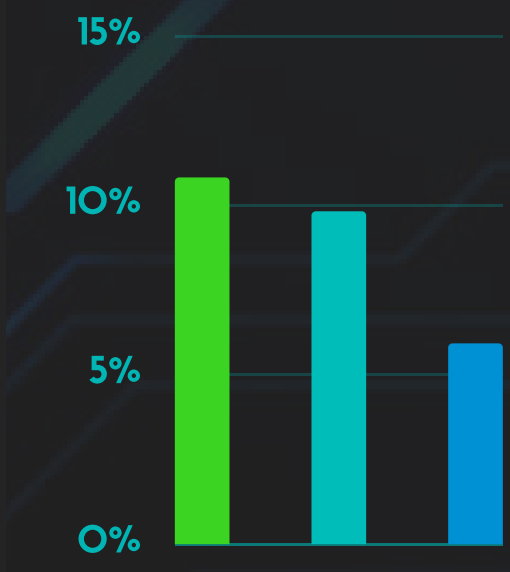
EL 27.5% ESTIMA QUE ES UNA LEY CON CONCEPTOS MUY ABIERTOS Y PELIGROSOS CON VACÍOS LEGALES.

POR TAL RAZÓN EL 18.6% OPINA QUE CARECE DE FUNDAMENTOS TÉCNICOS YA QUE CONSIDERAN NO HUBO PERIODO DE CONSULTAS CON LAS MÚLTPLES PARTES INVOLUCRADAS.



SIN EMBARGO EL 16.7% PIENSA QUE ES UNA BUENA INICIATIVA PARA CASTIGAR LOS ABUSOS COMETIDOS A TRAVÉS DE REDES SOCIALES.

POR OTRA PARTE EL 10.8% ASEGURA SE PIERDE LA LIBERTAD DE EXPRESIÓN Y LA PRIVACIDAD.



EL 10.8% SE MUESTRA ESCÉPTICO DE LA APLICACIÓN DE LA LEY.

MIENTRAS TANTO EL 9.8% NO SABE O PREFIERE NO OPINAR.

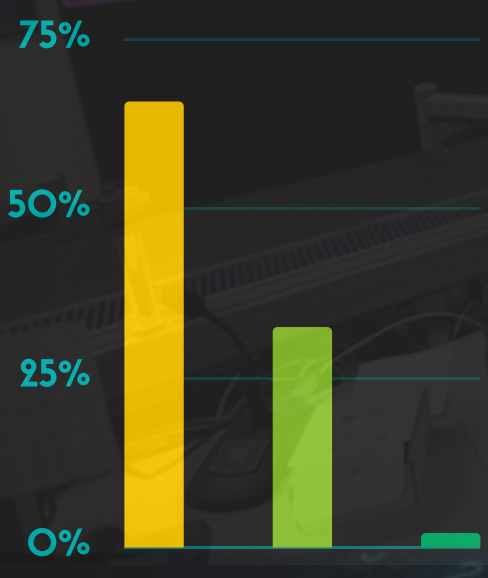
UNICAMENTE EL 5.9% CONSIDERA QUE PUEDE SER USADA PARA FINES POLÍTICOS.

www.nicaraguacibersegura.org
@defensoresdelcifrado
@nicaraguacibersegura
@nic_cibersegura

Nicaragua Cibersegura
Defensores del Cifrado.

LEYES RELACIONADAS AL USO DE INTERNET EN NICARAGUA

¿CONSIDERA USTED QUE LOS GOBIERNOS DEBEN TENER MECANISMOS TECNOLÓGICOS PARA ACCEDER A NUESTROS DATOS Y COMUNICACIONES? ¿POR QUÉ?

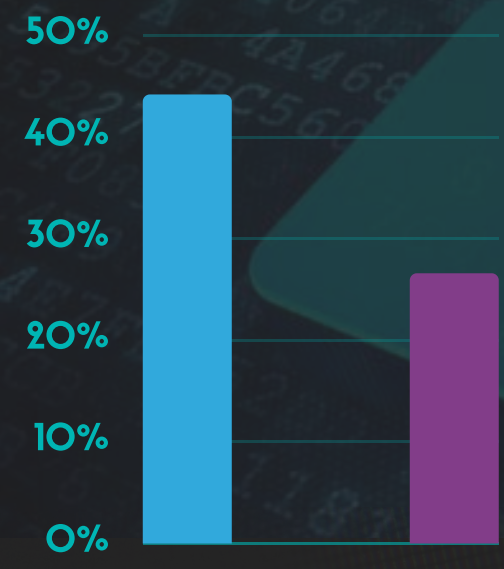


EL 65.7% CONSIDERA QUE NO, YA QUE ES SU PRIVACIDAD LA QUE ESTA EN JUEGO Y LOS GOBIERNOS USARÍAN ESTOS MECANISMO A SU FAVOR.

NO OBSTANTE EL 32.4% AFIRMA QUE SI, PERO DEBERÍA SER UNICAMENTE EN CASOS ESPECIALES PARA ATRAPAR A DELINCUENTES.

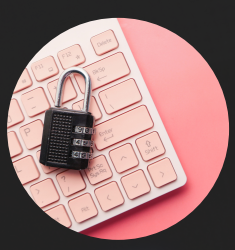
EL 2% NO SABE O PREFIERE NO OPINAR.

¿QUÉ MEDIDAS UTILIZAN PARA UNA NAVEGACIÓN SEGURA EN INTERNET?



EL 44.1% NO SE REGISTRA EN CUALQUIER PAGINA WEB O ENLACES EXTRAÑOS, ADEMÁS NO COMPARTE SU INFORMACIÓN PERSONAL.

CONSOLIDANDO RESPUESTAS EN UN ANÁLISIS FACTORIAL SE DETERMINA QUE EL 26.5% UTILIZA UNA O MÁS MEDIDAS COMO:



CONTRASEÑAS SEGURAS

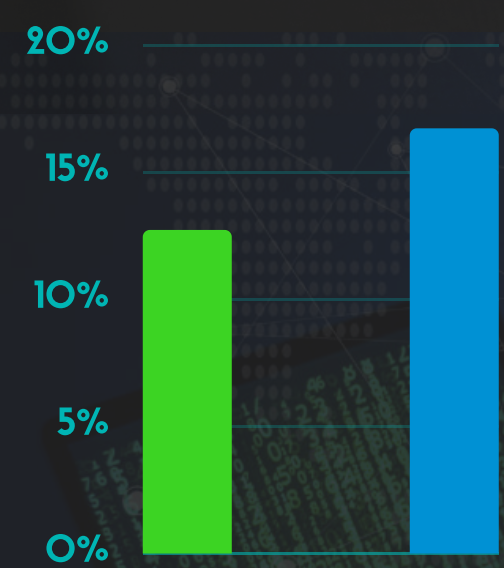
ANTIVIRUS Y ANTI SPYWARE

PROXY Y VPN

GESTIÓN DE LA PRIVACIDAD EN REDES SOCIALES.

FACTOR DE DOBLE AUTENTICACIÓN (2FA)

EVITAN CONECTARSE A REDES WIFI PUBLICAS



EL 12.7% EVITA LA COMUNICACIÓN CON EXTRAÑOS EN INTERNET.

EL 16.7% ADUCE QUE NO UTILIZA NINGUNA MEDIDA PARA PROTEGERSE EN INTERNET.

www.nicaraguacibersegura.org

@defensoresdelcifrado

@nicaraguacibersegura

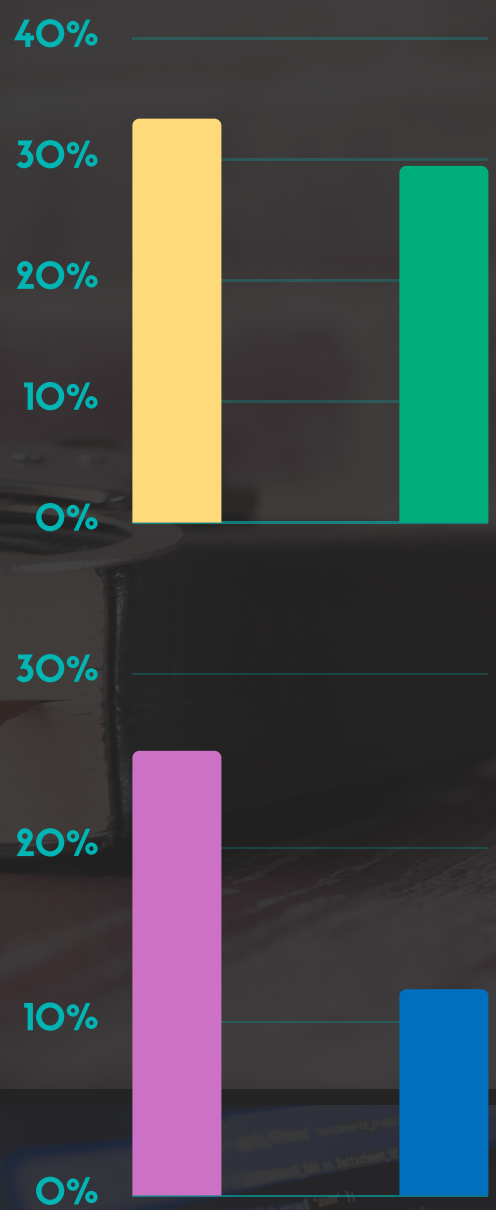
@nic_cibersegura

Nicaragua Cibersegura

Defensores del Cifrado.

LEYES RELACIONADAS AL USO DE INTERNET EN NICARAGUA

¿QUÉ PIENSAS DE LAS LEYES APROBADAS EN NICARAGUA RELACIONADAS CON LA TECNOLOGÍA EN MEDIO DE LA PANDEMIA?



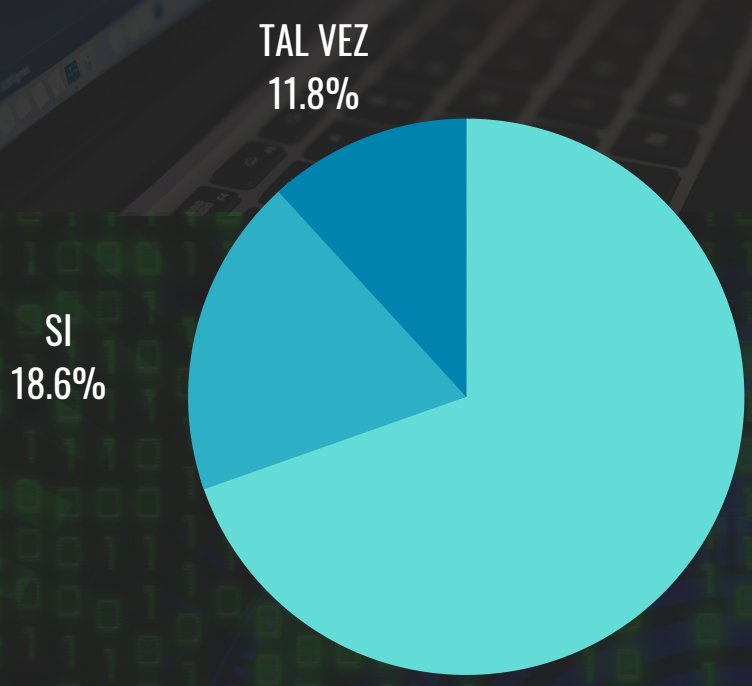
EL 29.4% CREE QUE APROVECHARON LA PANDEMIA PARA APROBAR LEYES QUE FAVORECEN AL GOBIERNO.

EL 33.3% NO SABE O PREFIERE NO DAR SU OPINIÓN AL RESPECTO DE ESTE TEMA.

EL 11.8% CONSIDERA QUE SE DEBIÓ CONSULTAR CON TODAS LAS PARTES INVOLUCRADAS, ANTES DE REDACTAR LA LEY.

CON LA PANDEMIA SE DIO MAYOR USO DE INTERNET Y CRECIERON LOS CIBERDELITOS. ERA NECESARIA UNA LEY. ES LO QUE OPINA EL 25.5% DE LOS ENCUESTADOS.

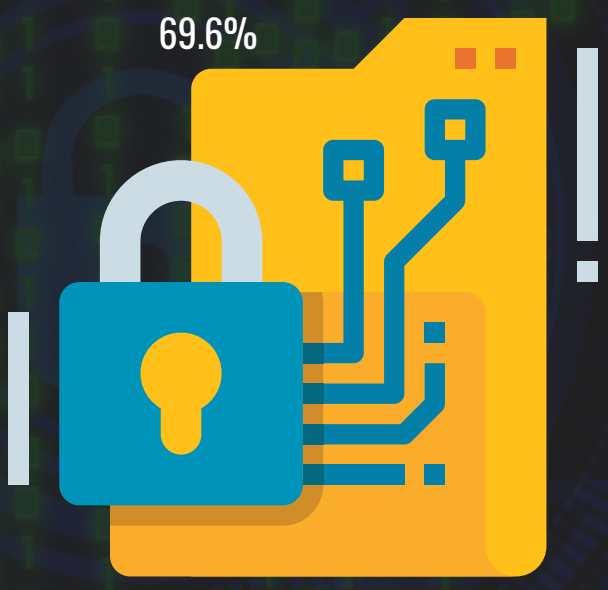
FINALIZANDO CON LA ENCUESTA, CONSULTAMOS SI LOS JÓVENES CONOCEN COMO CIFRAR SU SMARTPHONE O COMPUTADOR.



EL 69.6% ADMITE QUE NO SABE COMO HACERLO

EL 11.8% CONSIDERA QUE PUEDE SABERLO O LO HA REALIZADO SIN DARSE CUENTA.

EL 18.6% ASEGURA QUE SI SABE, COMO HACER ESTE PROCESO.



www.nicaraguacibersegura.org

@defensoresdelcifrado

@nicaraguacibersegura

@nic_cibersegura

Nicaragua Cibersegura

Defensores del Cifrado.