



GUÍA DE ACCIÓN SOBRE CONSIDERACIONES DE SEGURIDAD PERSONAL: TRABAJADORES DE INFRAESTRUCTURAS CRÍTICAS



INTRODUCCIÓN

En el actual entorno de amenazas, mantenerse alerta y asumir la responsabilidad de su seguridad personal es crucial para todos los trabajadores de infraestructuras críticas, tanto dentro como fuera del trabajo. Los trabajadores de infraestructuras críticas desempeñan una amplia variedad de servicios que operan, manejan y mantienen sistemas y activos fundamentales necesarios para la vida moderna estadounidense. Ser consciente de los riesgos o las amenazas asociados a su trabajo y seguir todos los procedimientos de seguridad le ayudará a protegerse a sí mismo, a sus allegados y a la infraestructura a la que presta servicio. La seguridad personal puede dividirse en tres partes principales: seguridad física, concienciación sobre la situación y seguridad en línea. Esta guía de acción no exhaustiva puede ayudarle a evaluar su postura ante la seguridad y le ofrece opciones a tener en cuenta para mitigar las amenazas.¹

EVALUACIÓN DE UN NIVEL DE PROTECCIÓN ADECUADO PARA LOS TRABAJADORES DE INFRAESTRUCTURAS CRÍTICAS

En esta guía encontrará un panorama general sobre cómo mantenerse seguro en casa, en el trabajo, en público y en línea. Depende de usted decidir qué medidas son las más adecuadas para su estilo de vida, sus vulnerabilidades de seguridad y las situaciones que pueda afrontar; por ejemplo, ciertos factores podrían aumentar el potencial de violencia en el lugar de trabajo:

- **Trabajar solo** o en lugares aislados.
- **Prestar servicios** o atención **en persona**.
- **Trabajar con materiales peligrosos** o información confidencial de seguridad nacional.
- **Responsabilidad por la protección** de la infraestructura crítica local o nacional.

Cuando evalúe sus necesidades de seguridad, tenga en cuenta lo siguiente:

- **Su ocupación y función profesional.** ¿Su trabajo o su profesión lo convierten en un objetivo llamativo?
- **Amenazas específicas.** ¿Existen pruebas creíbles que sugieran un riesgo para usted?
- **Su historia personal.** ¿Ha sido objeto de ataques o amenazas en el pasado?
- **Sus identificadores visuales personales.** ¿Muestra alguna afiliación a un grupo que lo convierta en un objetivo llamativo?

En la actualidad, los trabajadores de infraestructuras críticas se enfrentan potencialmente a una amplia gama de amenazas, desde actividades delictivas comunes hasta complot de grupos extremistas violentos. Si ha respondido afirmativamente a alguna o a todas las preguntas anteriores, esto podría indicar que usted y potencialmente otros empleados de infraestructuras críticas con los que trabaja están en riesgo y debería evaluar sus necesidades de seguridad. Cuando evalúe su seguridad personal, es importante que adopte un enfoque equilibrado y recuerde que debe tener en cuenta tanto su vida familiar como laboral: **observe sus prácticas y hábitos de seguridad personal y evalúe su entorno continuamente**. Las medidas que tome deben ser adecuadas en función de las amenazas percibidas. Un exceso de medidas de seguridad puede causar estrés e inconvenientes innecesarios; sin embargo, un esfuerzo insuficiente puede ponerlo en riesgo.

La capacidad de reconocer situaciones vulnerables es vital para evitarlas o estar preparado cuando ocurran. La vulnerabilidad es una característica física o un atributo de funcionamiento que hace que una entidad, un activo, un sistema, una red o una zona geográfica estén expuestos a la explotación o sean susceptibles a un peligro determinado.² Los atacantes son creativos cuando apuntan a sus objetivos. El objetivo de un atacante puede consistir en provocar vergüenza, molestias, angustia o puede tener la intención de causar lesiones físicas, perturbar el bienestar o amenazar vidas humanas.

1. ProtectUK. 2022. Publicly accessible locations (PALs) guidance: Personal security (Guía para ubicaciones de acceso público [PAL]: seguridad personal). Consultado el 8 de agosto de 2023. protectuk.police.uk/personal-security.

2. Departamento de Seguridad Nacional de EE. UU. (U.S. Department of Homeland Security). Risk Steering Committee (Comité Directivo de Riesgos). 2010. DHS Risk Lexicon, 2010 Edition (Léxico de riesgos del DHS). Consultado el 8 de agosto de 2023. cisa.gov/resources-tools/resources/dhs-risk-lexicon.

SEGURIDAD FÍSICA

PROTEJA SU HOGAR

Hay una variedad de medidas sencillas para tener en cuenta que pueden ayudarle a protegerse a sí mismo y a su hogar. Comience instalando o mejorando los sistemas de seguridad que rodean su residencia o propiedad. Asegure las puertas y ventanas con cerraduras, llaves, alarmas, luces y evalúe la posibilidad de instalar un sistema de circuito cerrado de televisión (CCTV, por sus siglas en inglés). Considere la posibilidad de utilizar un sistema de cierre avanzado para las entradas y ventanas con un sistema de videovigilancia supervisado (con capacidad de vistas múltiples).

Mantenga en buen estado las estructuras exteriores de la propiedad, como muros y vallas, y asegúrese de que todas las herramientas o escaleras que puedan utilizarse para acceder a su vivienda estén bien guardadas. Considere la posibilidad de retirar todo lo que pueda servir para causar daños, como ladrillos sueltos, piedras grandes y adornos de jardín. Asegúrese de cortar y mantener los arbustos, la maleza, etc. para que el follaje:

- **No se pueda utilizar** para que los intrusos se escondan o accedan a la vivienda.
- **No bloquee** la visión al exterior de las personas que se encuentran en el interior de la vivienda.

Asegure las puertas y ventanas exteriores con dispositivos de cierre adecuados, que pueden incluir mecanismos de cierre electrónicos y codificados. Lo mejor es tener un juego extra de llaves o códigos de entrada para utilizarlos en caso de emergencia. Considere la posibilidad de cambiar todo el sistema de cierre en caso de que los códigos de entrada se vulneren o se pierdan las llaves.

Invierta y mantenga en buen estado la iluminación exterior de modo que ilumine las puertas exteriores, las zonas de estacionamiento y los caminos alrededor de la casa. Considere la posibilidad de instalar cámaras que permitan ver las puertas y ventanas. Coloque estas luces y cámaras estratégicamente para eliminar los puntos ciegos en los que los intrusos podrían eludir la detección.

Si tiene un vehículo y no puede guardarlo en un garaje o en una zona cerrada, intente dejarlo a la vista del público. Estacionelo en una zona bien iluminada, a la vista de una cámara de CCTV o en un estacionamiento con vigilancia. Siempre cierre las ventanas, retire los objetos de valor de la vista y cierre el auto con llave, aunque solo se aleje unos minutos. Aprenda a utilizar el tipo de sistema de alarma antirrobo de su vehículo. Hay sistemas que incluyen notificaciones sonoras y visuales, además de servicios de localización de vehículos para agilizar la respuesta policial.

PLANIFICAR

Considere la posibilidad de elaborar un plan de acción de emergencia familiar y practicar lo que debe hacer en caso de emergencia. Para obtener ayuda para elaborar un plan, visite:

fema.gov/blog/have-emergency-plan-your-family.



ATAQUES CON ARMAS DE FUEGO

Un tirador activo es una o varias personas que matan o intentan matar a otras personas en una zona poblada.³ Los incidentes con tiradores activos suelen ser impredecibles y progresan con rapidez. En medio del caos, todos pueden desempeñar un papel fundamental a la hora de mitigar los efectos de un tirador activo.

Como las situaciones que involucran a un tirador activo suelen terminar en 10 o 15 minutos (antes de que las fuerzas policiales lleguen al lugar), las personas deben estar preparadas tanto mental como físicamente para responder a este tipo de incidentes.

En estos casos, considere la posibilidad de poner en práctica una estrategia de respuesta (como el paradigma “correr, esconderse, pelear”) según las políticas de seguridad de su organización. Se puede encontrar información y recursos adicionales en la página web de la Agencia de Seguridad Cibernética y de Infraestructura (CISA, por sus siglas en inglés) sobre [preparación para situaciones de tiradores activos](#).

EL FUEGO COMO ARMA

Los incendios intencionales se definen como cualquier incendio provocado o premeditado o intento de incendio (con o sin intención de cometer una estafa) de una vivienda, edificio público, vehículo de motor, aeronave u otros bienes personales.⁴ La motivación de quien provoca el incendio puede ser, entre otras, la venganza, el vandalismo, una estafa o el encubrimiento de delitos. Se pueden utilizar sustancias inflamables o un dispositivo pirotécnico improvisado (IID, por sus siglas en inglés) para iniciar el incendio.

La amenaza del fuego como arma puede resultar difícil de detectar antes de que comience el ataque. Debe saber cómo actuar si huele humo o ve que algo se prende fuego.

³ Oficina Federal de Investigaciones (Federal Bureau of Investigation), s. f. Active Shooter Safety Resources. Consultado el 1 de diciembre de 2023. fbi.gov/how-we-can-help-you/active-shooter-safety-resources.

⁴ Cybersecurity and Infrastructure Security Agency. 2021. Fire as a Weapon Action Guide. Consultado el 8 de agosto de 2023. cisa.gov/resources-tools/resources/fire-weapon-action-guide.

En caso de incendio, llame al 9-1-1 y siga las instrucciones del personal de emergencia. Abandone la zona del incendio de inmediato y alerte a los demás, si es posible. Evite las zonas donde pueda sentir olor a humo o ver fuego. Evacue las instalaciones interiores; cierre todas las puertas a su paso para contener el fuego. Si no puede evacuar, aléjese lo más posible del peligro y utilice los extintores según sea necesario. Tome conciencia de la situación y esté atento a actividades sospechosas o amenazas adicionales.

Consulte la [Guía de acción sobre el fuego como arma](#) de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) para obtener más consejos sobre cómo mitigar los casos en los que se utiliza el fuego como arma.

ARTEFACTOS EXPLOSIVOS IMPROVISADOS (IED)

Un artefacto explosivo improvisado (IED, por sus siglas en inglés) es un dispositivo colocado o fabricado de manera improvisada que incorpora sustancias químicas destructivas, letales, nocivas, pirotécnicas o inflamables y está diseñado para destruir, incapacitar, hostigar o distraer.⁵ Los artefactos explosivos improvisados varían, según los objetivos y los materiales disponibles, desde dispositivos pequeños y rudimentarios, como los dispositivos de sobrepresión o las bombas de tubo, rellenos en la mayoría de los casos de pólvora, hasta grandes artefactos transportados en vehículos que contienen grandes cantidades de explosivos.

Las amenazas pueden presentarse de diversas formas. Si alguna vez le preocupa una situación o un objeto sospechoso, llame inmediatamente a las fuerzas policiales locales. Los ejemplos que indican la existencia de una bomba pueden ser cables o componentes electrónicos inexplicables, otros componentes visibles similares a una bomba y sonidos, vapores u olores inusuales. Los incidentes en los que se sospecha la presencia de un artefacto explosivo improvisado requieren una respuesta del escuadrón de explosivos y la capacidad para diagnosticar y “neutralizar” dispositivos viables.

Para obtener más información sobre cómo reconocer objetos sospechosos, consulte [la ficha y el cartel “Objetos abandonados vs. objetos sospechosos”](#) y mire el video [“What to Do: Suspicious or Unattended Item”](#) (Cómo actuar: Objeto sospechoso o abandonado).

PROTESTAS Y MANIFESTACIONES

Independientemente de la misión o intención, mantenga la calma si se produce una protesta o manifestación pública cerca de su hogar, lugar de trabajo o incluso en su propiedad. Aunque las protestas puedan parecer intimidatorias, es poco probable que conlleven una amenaza física. Incluso si la situación se vuelve impredecible, mantenga la calma. Quédese adentro, cierre y bloquee puertas y ventanas, y corra las cortinas/persianas. Si se siente inseguro o la situación se agrava, llame a las fuerzas policiales.

Si es necesario, anote descripciones de las personas y los vehículos presentes. Facilite a la policía las grabaciones de videovigilancia, videos de teléfonos móviles o fotografías, ya que pueden ser útiles en caso de investigación.

La [hoja informativa Cómo proteger las infraestructuras durante manifestaciones públicas](#) de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) ofrece recomendaciones de seguridad para las empresas que puedan ser objeto de actos ilícitos durante manifestaciones públicas.

CONCIENCIA DE LA SITUACIÓN

La conciencia de la situación consiste en ser consciente de lo que ocurre a nuestro alrededor, tener en cuenta todos los factores y adaptar nuestro comportamiento para reducir el riesgo de lesiones para nosotros, nuestra familia o nuestros compañeros de trabajo.

VISITANTES

Siempre identifique a los visitantes antes de permitirles la entrada a su hogar. Considere la posibilidad de instalar una mirilla o una cámara en la puerta que le ayude a identificar quién se encuentra del otro lado de la puerta. Pida a los visitantes desconocidos que se identifiquen antes de abrir la puerta. Una vez dentro de su residencia, manténgalos cerca, preferiblemente delante de usted o en una posición en la que pueda observarlos. Procure tener un teléfono móvil a mano en todo momento.

MATERIALES CONFIDENCIALES

Siempre deseche o destruya adecuadamente el material confidencial que pueda tener información privada o de identificación personal (PII). La PII incluye todo tipo de información de carácter personal que pueda utilizarse para identificarlo.

SEGURIDAD PARA PEATONES

Priorice su seguridad personal cuando viaje, camine o corra en espacios públicos. Si toma las precauciones adecuadas, podrá reducir su vulnerabilidad y el riesgo de sufrir violencia o agresiones. Adopte medidas sencillas, como planificar una ruta segura, variar el recorrido cuando vaya a lugares habituales y evitar posibles puntos de peligro, como callejones poco transitados o mal iluminados, estacionamientos desiertos y alejados.

⁵ Departamento de Seguridad Nacional de EE. UU. Federal Bureau of Investigation. s. f. *Security and Resiliency Guide: Counter-Improvised Explosive Device (C-IED) Concepts, Common Goals, and Available Assistance*. Consultado el 8 de agosto de 2023. Página 4, cisa.gov/resources-tools/resources/security-and-resiliency-guide-srg-and-annexes.

Cuando esté en público, actúe con prudencia y tome precauciones para ocultar credenciales de trabajo o información personal. Tenga cuidado cuando porte credenciales o ingrese contraseñas en espacios públicos. Para obtener más datos y consejos, visite el sitio web sobre [Seguridad para peatones](#) de la Administración Nacional de Seguridad del Tráfico en las Carreteras.

MANTENGA LA CONCIENTIZACIÓN SITUACIONAL

Si se siente preocupado o inseguro en un lugar público, acérquese a un grupo de personas. Si no es posible, modifique sus movimientos para maximizar su conciencia de la situación y tome las siguientes precauciones:



- **Mantenga su teléfono móvil** listo para realizar una llamada de emergencia.
- **Esté alerta** y sea consciente de su ubicación exacta y sus alrededores.
- **Evite exhibir** joyas u objetos de valor.
- **Tenga en cuenta la iluminación de la zona, la ubicación y la proximidad** a otros comercios locales.
- **Cuando camine, colóquese de frente al tráfico que se aproxima** para evitar que los vehículos se acerquen por detrás.
- **Mantenga las manos libres** y permanezca atento a su entorno.
- **Evite hablar por teléfono**, usar auriculares o enviar mensajes largos.
- **Manténgase alerta** cuando camine y evite demorarse.
- **Cuando utilice un cajero automático**, evite exhibir el dinero en público.

SERVICIOS DE TRANSPORTE COMPARTIDO

Cuando utilice una aplicación de transporte compartido, procure informar a un amigo o compañero de trabajo sobre su ubicación y destino. Compruebe los datos del conductor y del vehículo antes de aceptar el viaje y subir al vehículo.

CÓMO RECONOCER Y DENUNCIAR ACTIVIDADES SOSPECHOSAS

Reconozca y denuncie las actividades sospechosas, como personas que merodean sin un motivo concreto alrededor de su hogar, lugar de trabajo o vehículo, o que intentan tomarle fotos de forma encubierta. Si observa que alguien abandona un objeto o paquete cerca de su hogar, lugar de trabajo o vehículo, infórmelo a la policía de inmediato. Obtenga más información sobre cómo denunciar actividades sospechosas visitando la campaña [“If You See Something, Say Something®”](#) (Si ve algo, diga algo).

DISPOSITIVOS DE PROTECCIÓN PERSONAL

Considere la posibilidad de portar un gas pimienta, una alarma sonora o un dispositivo de protección personal adicional para desorientar al agresor, avisar a los transeúntes y tener la oportunidad de escapar. Cuando sea posible, y de acuerdo con las leyes y reglamentaciones federales y locales, lleve y utilice dispositivos de protección personal.



Si se presta especial atención a las siguientes señales de advertencia y se notifican con rapidez, se puede contribuir a mitigar un posible incidente:

- **Amenaza verbal o escrita** contra usted, su hogar, sus pertenencias o su lugar de trabajo.
- **Sistemas y equipos** dañados o alterados.
- **Objetos sospechosos o abandonados:** bolsas, cajas, contenedores ocultos, etc., que puedan contener sustancias peligrosas.
- **Preguntas sospechosas** sobre los planos de los edificios, la ubicación de las entradas y salidas, los ascensores, los extintores, el suministro de agua y los sistemas de calefacción, ventilación y aire acondicionado (HVAC, por sus siglas en inglés).
- **Cantidades o ubicaciones inusuales de materiales inflamables o combustibles**, como productos inflamables, pinturas, desengrasantes, limpiadores a base de alcohol, aerosoles y tanques de gas propano.
- **Mensajes en redes sociales** que promuevan imágenes o ideas para cometer atentados.

Consulte los [indicadores y ejemplos de denuncia de actividades sospechosas](#) para obtener más información.

ENFRENTAMIENTOS

Una situación de enfrentamiento puede ser estresante. Debe centrarse en los comportamientos observables que puedan ser indicativos de violencia potencial. En estas situaciones, es importante mantener la calma y evaluar la situación para determinar si es seguro intervenir. Tenga en cuenta los límites de sus capacidades y solicite ayuda al personal de seguridad o a las fuerzas policiales apenas sea seguro hacerlo.

Si está capacitado y es idóneo, procure distender de forma segura las situaciones de tensión mediante acciones deliberadas que incluyan la escucha y comunicación efectivas. Recuerde que la “distensión” no es algo que se hace; es el objetivo.

Consulte la [Serie sobre técnicas de distensión de la Agencia de Seguridad Cibernética y de Infraestructura \(CISA\)](#) para obtener consejos sobre cómo mantenerse alerta y desenvolverse en situaciones potencialmente hostiles.

VEHÍCULOS DE MOTOR Y VIAJES

Antes de salir de su hogar o lugar de trabajo, mire a su alrededor y tome nota de vehículos sospechosos que puedan estar al acecho o merodeando. Inspeccione la zona alrededor del vehículo en busca de elementos que no deban estar sobre o cerca de su vehículo. Si ocurriera algún incidente, esta información podría ser útil para la policía.

Si es posible, evite repetir patrones durante sus traslados para que los posibles malhechores no puedan predecir su ubicación. Cambie sus recorridos y varíe los horarios de salida tanto como le sea posible. Asegúrese de que todas las puertas y el maletero del vehículo permanezcan cerrados durante el viaje. Abra las ventanas lo suficiente para ventilar. Conduzca con precaución y mantenga una distancia prudencial con el vehículo de adelante. Además, siempre asegúrese de que su vehículo tenga suficiente combustible (o, si es eléctrico, que tenga suficiente carga) para el viaje.

Si cree que lo están siguiendo, trate de mantener la calma y su vehículo en movimiento. Cierre todas las ventanas y asegúrese de que las puertas están bloqueadas. Póngase en contacto con las fuerzas policiales de inmediato. Si puede, diríjase a la estación de policía más cercana, no conduzca hasta su casa. Intente anotar el número de matrícula, la marca y el modelo de todo vehículo sospechoso.

Si tiene un choque o un desperfecto mecánico, observe su entorno y contacte inmediatamente al personal de emergencia y al servicio de remolque de vehículos. Siga las instrucciones de las autoridades policiales.

LLAMADAS TELEFÓNICAS Y AMENAZAS ANÓNIMAS⁶

Las llamadas telefónicas y amenazas anónimas suelen tener como objetivo causar miedo, alarma y angustia. Recuerde hacer siempre lo siguiente:

- **Mantenga la calma** y NO cuelgue el teléfono.
- **Retenga a la persona que llama en la línea** el mayor tiempo posible. Sea cortés y muestre interés para que sigan hablando. Pueden revelar información importante que puede ser útil en caso de investigación policial.
- Si es posible, **haga una señal o pase una nota** a las otras personas que estén a su alrededor para que escuchen y ayuden a avisar a las autoridades.
- **Anote** toda la información posible: número de identificación de la persona que llama, formulación exacta de la amenaza, tipo de voz o comportamiento, etc., que ayude a los investigadores.
- Si es posible y está legalmente permitido, **grabe la llamada**.

Hacer llamadas telefónicas para amenazar u hostigar está prohibido por la ley federal. Si recibe alguna llamada de este tipo, póngase en contacto con las fuerzas policiales locales. Además, puede denunciar la amenaza a la Agencia Federal de Investigaciones (FBI, por sus siglas en inglés). Consulte la [Guía de intimidación ante amenazas del FBI](#) para obtener consejos.

Como la mayoría de las amenazas de bomba se hacen por teléfono, consulte la [Lista de verificación de amenazas de bomba del Departamento de Seguridad Nacional \(DHS, por sus siglas en inglés\)](#) y la [Guía de amenazas de bomba de la Agencia de Seguridad Cibernética y de Infraestructura \(CISA\)](#), que ofrecen instrucciones sobre cómo responder a una amenaza de bomba, así como una lista completa de información que ayudará a las fuerzas policiales en la investigación de una amenaza de bomba.

SEGURIDAD EN LÍNEA

Solo instale aplicaciones de “tiendas de aplicaciones” de confianza para evitar descargas potencialmente maliciosas. No descargue aplicaciones de fuentes desconocidas o no verificables. Tenga en cuenta qué permisos se conceden a las aplicaciones para acceder a otra información de su teléfono.

Cree y mantenga una contraseña segura que sea única para cada uno de sus dispositivos o cuentas y use un administrador de contraseñas para organizarlos. Active la autenticación multifactor (MFA, por sus siglas en inglés) para cada cuenta o aplicación que la ofrezca. Habilitar la MFA ayuda a proteger información personal, como su correo electrónico, redes sociales, información financiera y otra información importante.

En su navegador web, busque localizadores uniformes de recursos (URL, por sus siglas en inglés) que comiencen con “https” (una indicación de que los sitios usan cifrado) en lugar de “http”. El Protocolo seguro de transferencia de hipertexto (HTTPS, por sus siglas en inglés) es un protocolo de comunicación de internet que se usa para cifrar y transmitir de forma segura información entre el navegador web de un usuario y el sitio web al que está conectado. Está diseñado para proteger mejor la integridad y confidencialidad de la información de los usuarios cuando visitan sitios web.⁷

Consulte [Secure Our World de Agencia de Seguridad Cibernética y de Infraestructura \(CISA\)](#) para obtener más información sobre cómo mantenerse seguro en línea.

ACTUALIZACIONES DE SOFTWARE

Mantenga el software actualizado para que los atacantes no puedan aprovechar información confidencial o vulnerabilidades. Muchos sistemas operativos ofrecen actualizaciones automáticas. Si esta es una opción, active las actualizaciones automáticas en la configuración de seguridad de la aplicación del dispositivo.



⁶ Federal Bureau of Investigation. s. f. Threat Intimidation Guide. Consultado el 8 de agosto de 2023. [fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view](https://www.fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view).

⁷ Departamento de Seguridad Nacional de EE. UU. 2018. Protocolo seguro de transferencia de hipertexto (HTTPS). Consultado el 12 de febrero de 2024. cisa.gov/resources-tools/resources/hyper-text-transfer-protocol-secure-https.

USO DE DISPOSITIVOS ELECTRÓNICOS

Los dispositivos y las redes móviles pueden contener diversos datos personales, como información bancaria en línea, correos electrónicos, mensajes de texto, contactos, redes sociales y fotografías. Para mantener su dispositivo seguro, utilice todas las funciones de seguridad y asegúrese de actualizar el software del dispositivo de manera constante. Cree contraseñas seguras para el teléfono y las tarjetas SIM y desactive los servicios de localización innecesarios.⁸

Siempre cambie el PIN predeterminado para acceder al buzón de voz. Procure limitar los servicios de localización en su teléfono y revise la configuración de privacidad para evitar que otras personas rastreen sus movimientos e identifiquen su domicilio o lugar de trabajo a través de aplicaciones de terceros. Revise las protecciones de privacidad y seguridad de [Apple](#) y [Android](#) para mejorar la seguridad de sus dispositivos.

REDES SOCIALES

Internet puede ser una valiosa fuente de información, educación y entretenimiento. Sin embargo, es necesario mantenerse alerta y tomar precauciones para limitar la cantidad de información personal que se publica en Internet, especialmente en las redes sociales.

Las redes sociales más populares permiten crear un perfil personal e interactuar con otras personas en línea. En los sitios de redes empresariales, la gente puede añadir más detalles a sus perfiles e incluir sus antecedentes laborales y otra información general. Aunque estas herramientas le ayudan a comunicarse con los demás y a publicitar su trayectoria profesional, publicar información personal en línea presenta riesgos potenciales.

Tenga cuidado al publicar información personal. Los agentes maliciosos pueden utilizar los datos de localización de fotos, cumpleaños, nombres completos, domicilios particulares y detalles del correo electrónico cuando jaquean o cometen robos de identidad. Además, la información sobre el empleo, los miembros de la familia, las aficiones o los detalles del vehículo son valiosos para los delincuentes y enemigos. Su familia y amigos también pueden compartir información sobre usted sin querer si no toman las medidas adecuadas para proteger la información de su propio perfil. Recuerde que en internet no existe un botón de “eliminar”. Compártalo con cuidado, porque incluso si elimina una publicación o una imagen de su perfil, es probable que alguien aún la vea.

Algunas redes sociales son propietarias de los datos que publica y los venden a terceros. Revise con frecuencia su configuración de privacidad y etiquetado de lugares en estos sitios; de lo contrario, está en riesgo de que una gran audiencia, sin que usted lo sepa, vea parte o todo su perfil personal.^{9, 10}

- ⁸ Comisión Federal de Comunicaciones. 2019. Protect Your Smart Device (Proteja su dispositivo inteligente). Consultado el 20 de septiembre de 2023. [fcc.gov/consumers/guides/protect-your-mobile-device](https://www.fcc.gov/consumers/guides/protect-your-mobile-device).
- ⁹ Gobierno del Reino Unido. National Cyber Security Centre. 2019. Social Media: how to use it safely (Redes Sociales: cómo usarlas de forma segura). Consultado el 20 de septiembre de 2023. [ncsc.gov.uk/guidance/social-media-how-to-use-it-safely](https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely).
- ¹⁰ Cybersecurity and Infrastructure Security Agency, National Cyber Alliance. 2019. Social Media Cybersecurity (Ciberseguridad en redes sociales). Consultado el 20 de septiembre de 2023. [cisa.gov/sites/default/files/publications/NCSAM_SocialMediaCybersecurity_2020.pdf](https://www.cisa.gov/sites/default/files/publications/NCSAM_SocialMediaCybersecurity_2020.pdf).

REVISIÓN DE LA CONFIGURACIÓN DE UBICACIÓN Y PRIVACIDAD DE LAS REDES SOCIALES

X, anteriormente conocida como Twitter

- twitter.com/settings/privacy_and_safety
- twitter.com/settings/location_information

Instagram

- help.instagram.com/811572406418223
- **IOS:** help.instagram.com/171821142968851
- **Android:** En su dispositivo Android, navegue a Configuración > Aplicaciones > Instagram > Permisos > Ubicación

Facebook

- facebook.com/help/325807937506242/
- facebook.com/help/337244676357509

Snapchat

- help.snapchat.com/hc/en-gb/sections/5690164367636-Privacy-Settings
- help.snapchat.com/hc/en-us/articles/7012322854932-How-do-I-turn-on-Ghost-Mode

TikTok

- tiktok.com/safety/en/privacy-and-security-on-tiktok/
- support.tiktok.com/en/account-and-privacy/account-privacy-settings/location-services-on-tiktok



DOXEO

El doxing se refiere a la práctica de recopilar información de identificación personal (PII, por sus siglas en inglés) de una persona (o información confidencial de una organización) de fuentes abiertas o materiales comprometidos y divulgarla públicamente o usarla con fines maliciosos.^{11, 12} Los delincuentes pueden usar esta información para chantajear o para incitar el miedo en objetivos potenciales.

Al publicar en línea, es importante ser consciente de lo que se publica y de cómo se publica. Si publica demasiada información sin aplicar la configuración de privacidad adecuada, es posible que esté poniendo en peligro su seguridad personal. Los demás pueden utilizar esta información para crear una imagen de sus relaciones, opiniones, lugares de interés y otros temas que pueden aprovechar en el futuro.

Los corredores de datos también pueden recopilar esta información personal y venderla a otras compañías. Para minimizar que sus datos lleguen a los corredores:

- **Evite** compartir PII.
- **No** acepte en las redes sociales a personas que no conoce en la vida real.
- **Asegúrese de que** las aplicaciones que usa tengan cifrado de extremo a extremo.
- **Limite** los permisos de las aplicaciones.
- **Configure** alertas de Google para su nombre.
- **Considere tomarse el tiempo** para elegir no participar en los principales corredores de datos y sitios de búsqueda de personas o suscribirse a un servicio que lo haga por usted.

La información basada en la ubicación puede publicarse en las redes sociales, especialmente desde teléfonos móviles y dispositivos móviles con GPS. Esta información no es segura y puede verla cualquier persona, incluso las que podrían desear hacerle daño. Controle lo que publica y hágalo de forma responsable para no poner en peligro a nadie.

Si cree que es víctima de doxeo, haga lo siguiente:

- **Informe el incidente** a las autoridades locales y a cualquier plataforma en línea donde se podría haber divulgado su información personal.
- **Documente** lo ocurrido y haga capturas de pantalla para compartirlas con los investigadores.
- **Determine** qué información se utilizó, la gravedad de la amenaza y el indicador de compromiso.
- **Colabore con los administradores de los sitios web** para eliminar información de sitios web o aplicaciones.
- **Configure los ajustes de privacidad** con las opciones que otorgan más privacidad.
- **Manténgase atento a los indicios** de robo de identidad, controle las cuentas financieras, establezca alertas de fraude y cambie la información de acceso y contraseña de todas las cuentas en línea.

Las leyes contra el doxing varían según la jurisdicción, por lo que es importante buscarlas en su área mientras considera las opciones de reducción y prevención. Si le preocupa su seguridad física, póngase en contacto con las fuerzas policiales locales para informarse de las medidas a tomar.

RECONOZCA Y DENUNCIE LA SUPLANTACIÓN DE IDENTIDAD

Los delincuentes suelen usar tácticas de suplantación de identidad para que usted abra enlaces, correos electrónicos o archivos adjuntos dañinos que podrían solicitar su información personal o infectar sus dispositivos. Estos mensajes suelen estar diseñados para que usted crea que provienen de una persona u organización de confianza.

Los mensajes de suplantación de identidad suelen llegar como correo electrónico, mensaje de texto, mensaje directo en las redes sociales o una llamada telefónica. Tenga cuidado con el lenguaje urgente o emotivo, las solicitudes de envío de información personal, los URL acortados que no sean de confianza y las direcciones de correo electrónico y enlaces incorrectos.

Si sospecha que ha sido víctima de un intento de suplantación de identidad, no haga clic en ningún enlace ni archivo adjunto. En su lugar, denúncielo y luego elimine el mensaje.

11. Departamento de Seguridad Nacional de EE. UU. 2024. Oficina de Alianzas y Participación (Office of Partnership and Engagement). Resources for Individuals on the Threat of Doxing (Recursos para personas sobre la amenaza del doxing). Consultado el 9 de febrero de 2024. dhs.gov/publication/resources-individuals-threat-doxing.

12. Organización Europea para la Investigación Nuclear. 2017. Computer Security: Enter the next level: Doxware (Seguridad informática: Entramos al siguiente nivel: Doxware). Consultado el 12 de diciembre de 2023. home.cern/news/news/computing/computer-seguridad-entrar-al-siguiente-nivel-doxware.

RECURSOS

SEGURIDAD FÍSICA

- [Guía de seguridad y resiliencia de la CISA](#)
- [Preparación contra tiradores activos de la CISA](#)
- [Guía de intimidación por amenazas del FBI](#)
- [Amenazas de bomba de la CISA](#)
- [Serie sobre técnicas de distensión de la CISA](#)

CONCIENCIA DE LA SITUACIÓN

- [Centro de Prevención, Concientización y Recursos contra el Acoso \(SPARC, por sus siglas en inglés\)](#)

SEGURIDAD EN LÍNEA

- [Secure Our World de la CISA](#)
- [Privacidad y aplicaciones para dispositivos móviles de la CISA](#)
- [CISA Insights: Mitigating the Impacts of Doxing on Critical Infrastructure \(Perspectivas de la CISA: cómo mitigar los impactos del doxeo en la infraestructura fundamental\)](#)
- [CISA Social Media Cybersecurity \(Ciberseguridad en redes sociales de la CISA\)](#)