



BOLETÍN DE NOTICIAS DEL CONSUMIDOR DE LA FLORIDA

Julio 2025

Una Publicación del Departamento de
Agricultura y Servicios al Consumidor

¿VIGILANCIA O ADVERTENCIA?

Conocer la diferencia entre una vigilancia y una advertencia puede ayudarle a mantenerse a salvo. Ya sea una vigilancia o una advertencia, escuche atentamente las instrucciones de los funcionarios locales usando un televisor, radio, teléfono celular u otro dispositivo de comunicación.

Alerta de Tormenta Tropical: Un anuncio de que las condiciones de tormenta tropical (vientos sostenidos de 39 de 73 mph) son posibles dentro del área especificada dentro de 48 horas.

Advertencia de Tormenta Tropical: Un anuncio de que se esperan condiciones de tormenta tropical (vientos sostenidos de 39 a 73 mph) dentro del área especificada dentro de las 36 horas.

Alerta de Huracán: Un anuncio de que las condiciones de huracán (vientos sostenidos de 74 mph o más) son posibles en algún lugar dentro del área especificada. Debido a que las actividades de preparación para huracanes se vuelven difíciles una vez que los vientos alcanzan la fuerza de tormenta tropical, la alerta de huracán se emite 48 horas antes del inicio anticipado de los vientos con fuerza de tormenta tropical.

Advertencia de Huracán: Un anuncio de que se esperan condiciones de huracán (vientos sostenidos de 74 mph o más) en algún lugar dentro del área especificada. Debido a que las actividades de preparación para huracanes se vuelven difíciles una vez que los vientos alcanzan la fuerza de tormenta tropical, la advertencia de huracán se emite 36 horas antes del inicio anticipado de los vientos con fuerza de tormenta tropical.

Alerta de Tornado: Es posible que se produzcan tornados en el área de vigilancia y cerca de ella. Esté preparado para actuar rápidamente si se emite una advertencia.

Advertencia de Tornado: Un tornado ha sido avistado o indicado por el radar meteorológico. Diríjase a una habitación segura de inmediato.

Alerta de Inundación: Se emite una alerta de inundación cuando las condiciones son favorables para la inundación. No significa que se vayan a producir inundaciones, pero es posible.

Advertencia de Inundación: Se emite una advertencia de inundación cuando la inundación es inminente o está ocurriendo.

Advertencia de Inundación Repentina: Se emite una advertencia de inundación repentina cuando una inundación repentina es inminente o está ocurriendo. Si se encuentra en un área propensa a inundaciones, muévase inmediatamente a un terreno elevado. Una inundación repentina es una inundación repentina y violenta que puede tardar minutos u horas en desarrollarse.

¿BUSCA UNA BANDERA ESTADOUNIDENSE HECHA EN LOS EE. UU.? ¡ESTO ES LO QUE DEBES SABER!

Cuando se trata de comprar una bandera estadounidense, hay mucho para elegir. No todos están hechos en los EE. UU. Si está buscando uno que lo sea, esto es lo que debe tener en cuenta.

Las banderas importadas deben tener etiquetas que indiquen dónde se fabricaron. Por lo tanto, si vas a comprar en una tienda, echa un vistazo a la etiqueta del producto. En línea, es posible que no encuentres esta información, especialmente si estás comprando una bandera más pequeña. En su lugar, fíjate en dónde se encuentra el vendedor: busca la dirección en los términos de servicio o la política de privacidad del sitio web. Si la tienda está en el extranjero, es muy probable que sus productos no estén hechos en los EE. UU. También tómese el tiempo para leer las reseñas. ¿El vendedor tiene buena reputación? Busca en línea el nombre del vendedor y términos como “revisión”, “queja” o “estafa”. Vea lo que otras personas tienen que decir.

¿Y qué pasa si un vendedor dice que su bandera estadounidense “[se envía desde los EE. UU.](#)”? Eso no significa necesariamente que se haya fabricado en los Estados Unidos. Algunas tiendas envían productos importados a los centros de distribución de EE. UU. para su almacenamiento y procesamiento antes de enviárselos.

Finalmente, sepa que incluso si compra con cuidado, los estafadores están ahí fuera. Es posible que haga clic en “comprar” y nunca obtenga su bandera. O tal vez aparezca una bandera, pero no es lo que esperabas. Pagar con tarjeta de crédito, si puedes, te ayuda a protegerte si pagas por algo y nunca llega. Y si crees que alguien está tratando de hacer pasar una bandera como Made in the USA cuando no lo es, repórtalo a la FTC en [ReportFraud.ftc.gov](https://www.ftc.gov/ReportFraud).

Para obtener más consejos sobre cómo comprar de forma segura, lea [Online Shopping](#).



CÓMO RECONOCER UNA ESTAFA FALSA DE RENOVACIÓN DE CONTRATO DE GEEK SQUAD

Los estafadores vuelven a la carga, haciéndose pasar por empresas conocidas e intentando estafar a la gente. Esta vez se hacen pasar por Geek Squad, el servicio de soporte técnico de Best Buy. Esto es lo que escuchamos sobre la estafa y qué hacer si la ve.

Recibe un mensaje de texto o correo electrónico que dice que le cobraron o le cobrarán cientos de dólares para renovar su membresía de Geek Squad. Si desea disputar el cargo o cancelar su membresía, el mensaje dice que debe llamar a un número de teléfono dentro de las 24 horas.

Si llamas al número, lo que no debes hacer, es posible que el estafador te pida acceso remoto a tu computadora. Si se lo da, pueden instalar programas espía en su computadora, robar sus credenciales de banca en línea y drenar dinero de su cuenta bancaria.

Algunos estafadores pueden pedirle la información de su cuenta bancaria para reembolsar su dinero, luego falsificar una transacción y hacer que parezca que accidentalmente le reembolsaron demasiado. Para devolverles el dinero, le dicen que compre tarjetas de regalo y les dé los números de las tarjetas de regalo y los PIN.

Los estafadores envían mensajes alarmantes como este para molestarlo. No se lo permitas. Si crees que el mensaje es legítimo, comunícate con la compañía en cuestión usando un número de teléfono que sepas que es real. **No Utilice el Número Incluido en el Mensaje.**

También revise su tarjeta de crédito o cuenta bancaria para ver si hay una transacción no autorizada. Si ves uno, repórtalo a la institución y pídeles que lo reviertan y te devuelvan tu dinero.

Averigüe qué hacer si [le pagó a un estafador](#) o le dio [su información personal](#) o [acceso a su computadora](#).

Si ve una estafa, repórtela a la FTC en [ReportFraud.ftc.gov](https://www.ftc.gov/ReportFraud).



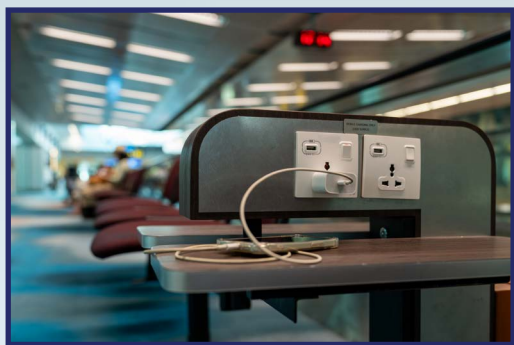
SEGURIDAD DEL DISPOSITIVO CUANDO SE VIAJA

Si planea viajar pronto, es probable que lleve su teléfono celular u otro dispositivo portátil, como su tableta, o varios dispositivos electrónicos. Incluso con la biometría, como las huellas dactilares y el reconocimiento facial, y los códigos de acceso, contraseñas y patrones para mantener su información segura, aún podría ser vulnerable al robo de datos o de identidad.

Seguridad Bluetooth

Bluetooth se usa para conectar sus dispositivos móviles a auriculares inalámbricos, habilitar llamadas con manos libres mientras conduce e incluso escuchar su lista de reproducción favorita en el automóvil. Un usuario debe permitir una conexión Bluetooth antes de que se compartan los datos (lo que se denomina “emparejamiento”), lo que proporciona cierto grado de seguridad de los datos, pero pone en riesgo sus datos personales. Al usar Bluetooth, hay algunos pasos que puede seguir para proteger sus datos:

- Apaga el Bluetooth cuando no lo estás usando. Cuando lo mantiene activo, los piratas informáticos pueden descubrir otros dispositivos que se han conectado antes y luego falsificar esos dispositivos para obtener acceso a sus datos.
- Si alquilas un coche y emparejas tu dispositivo móvil con él, asegúrate de desvincular y borrar todos los datos personales cuando devuelvas el coche. Haz lo mismo si vendes un coche con Bluetooth.
- Para evitar que dispositivos desconocidos descubran su conexión Bluetooth, use Bluetooth en modo “oculto”, no en modo “detectable”.



¿Qué es el Juice Jacking?

Esas estaciones de carga que encuentra en aeropuertos, restaurantes y vestíbulos de hoteles pueden ser convenientes, pero podría estar exponiéndose al robo cibernético. Esta actividad se conoce como “juice jacking”.

Las estaciones de carga USB de uso público podrían cargar programa maligno en su dispositivo mientras se carga, dando a los ladrones acceso directo a sus datos personales y contraseñas. Esos datos pueden venderse en línea a otros delincuentes retorcidos o usarse para acceder a sus cuentas en línea.

¿Cómo puede proteger sus dispositivos contra el robo de jugo?

- Utilice tomas de corriente de CA cuando cargue la carga; Traiga su propio ladrillo de carga y cables y cargue sus artículos usando un tomacorriente de pared estándar.
- Utilice una batería externa. El uso de una batería externa recargable le permite cargar sobre la marcha.
- Utilice un cable de solo carga. Estos cables evitan que los datos se envíen o reciban durante la carga. Asegúrate de comprar a un proveedor de confianza.
- Ten cuidado. Cuando cargues tu dispositivo en una estación de carga de uso público, si ves un mensaje que te pregunta si quieres “compartir datos” o “confiar en esta computadora” o “solo cargar”, asegúrate de seleccionar “solo cargar”.



Wi-Fi Público

Si eliges usar redes Wi-Fi públicas para acceder a Internet cuando viajas, hazlo con precaución. Los piratas informáticos pueden acceder a la conexión y obtener información sobre los datos de su dispositivo y sus cuentas en línea. Puede utilizar los siguientes consejos para mitigar el riesgo:

- Verifica los puntos de acceso Wi-Fi disponibles. Consulte con el personal del establecimiento para asegurarse de que está utilizando el punto de acceso correcto, no un estafador que intenta robar sus datos.
- Busque “https” cuando comparta datos a través de cualquier red. Los sitios web que comienzan con “https” cifran sus datos cuando se transmiten.
- Instale una aplicación (de buena reputación) en su dispositivo para obligar a los navegadores web a utilizar el cifrado al conectarse a sitios web.
- Asegúrese de que su dispositivo no se conecte automáticamente a redes Wi-Fi cercanas cuando esté dentro del alcance.
- Utilice una VPN (red privada virtual) si utiliza con frecuencia puntos de acceso públicos. La VPN encripta todas las transmisiones entre Internet y su dispositivo.
- Use su plan de datos en lugar de un punto de acceso cuando comunique información confidencial a través de Internet.

PROTECCIÓN DE SU INFORMACIÓN PERSONAL

Cuando se trata de proteger su identidad, puede pensar en guardar los nombres de usuario para usted, usar contraseñas seguras y revisar sus estados de cuenta. Todo eso es genial. Pero también es importante pensar en lo que haces con los documentos o archivos digitales que contienen tu información financiera. Entonces, veamos lo que debe conservar y bloquear, y lo que debe triturar o eliminar.

Conservar Durante un Año

- Estados de cuenta
- Comprobantes de pago
- Facturas médicas indiscutibles
- Tarjetas de crédito y facturas de servicios públicos
- Cheques depositados

Si puede acceder a estos documentos electrónicamente, considere triturar sus copias impresas.

Conservar Durante al Menos Tres Años

- Declaraciones de impuestos sobre la renta
- Documentos relacionados con los impuestos, como cheques cancelados, recibos, formularios W-2 y formularios 1099
- Registros relacionados con la venta de una casa

En algunos casos, el [IRS recomienda](#) conservar las declaraciones de impuestos y los documentos relacionados con los impuestos durante más de tres años. Si puede acceder a estos documentos electrónicamente, considere triturar sus copias impresas.

Guárdalo Mientras le Pertenezca

- El título de propiedad de su vehículo
- El título o escritura de su casa
- Documentos relacionados con préstamos hipotecarios o vehiculares
- Recibos de mejoras para el hogar
- Contratos de alquiler y arrendamientos
- Recibos de compra e información de garantía para electrodomésticos principales

Conservar para Siempre

Y guardar bajo seguridad:

- Certificado de nacimiento o documentos de adopción
- Tarjetas de Seguro Social
- Pasaportes válidos y documentos de ciudadanía o residencia
- Licencias de matrimonio y sentencias de divorcio
- Expedientes militares
- Testamentos, testamentos vitales, poderes notariales y planes de jubilación y pensiones
- Certificados de defunción de los miembros de la familia
- Registros de salud vitales (especialmente aquellos que son anteriores a los registros de salud electrónicos)

Triturar

- Recibos de cajeros automáticos
- Ofertas de crédito o seguro
- Cheques compensados (después de 14 días)
- Informes de crédito
- Información sobre las recetas de los medicamentos que ya no toma
- Garantías vencidas
- Tarjetas de crédito, licencias de conducir y otras formas de identificación vencidas

Cuando llegue el momento de deshacerse de los documentos con su información personal o financiera, trítúrelos. Si no tienes una trituradora, busca un día de trituración local en tu comunidad. Averigüe qué más puede hacer para [protegerse del robo de identidad](#).

FACEBOOK Y LAS ESTAFAS DE INVERSIÓN EN REDES SOCIALES

Una coalición bipartidista de 42 fiscales generales de todo Estados Unidos instó recientemente a la empresa matriz de Facebook, Meta, a reducir el aumento de las estafas de inversión en Facebook y WhatsApp.

La estafa se dirige a los usuarios de Facebook con anuncios en los que aparecen inversores de renombre, como Warren Buffett o Elon Musk, que ofrecen al usuario la oportunidad de convertirse en miembro de un grupo de chat de inversión a través de WhatsApp, una aplicación de mensajería propiedad de Meta. Sin embargo, esos inversores famosos no forman parte del grupo de chat y las recomendaciones para comprar penny stocks son de malos actores que esperan beneficiarse del esquema de bombeo y descarga. La compra de estas acciones aumenta el valor ("bombeo"), luego el instigador vende los valores a un precio artificialmente alto ("volcado"), lo que hace que el valor se desplome.

Si estás pensando en invertir, recuerda los siguientes consejos:

- Investigue a fondo antes de invertir. Busque el nombre de la empresa o el nombre de la criptomoneda en línea utilizando términos adicionales como "revisión", "estafa" o "queja" en la barra de búsqueda.
- Nunca dé la información de su cuenta (tarjeta de crédito o cuenta bancaria) hasta que investigue la inversión.
- Desconfíe de las propuestas de inversión en las plataformas de redes sociales.
- No confíe en consejos de inversión o secretos en tableros de mensajes en línea. Los sitios enlazados pueden ser sitios web falsos que promueven lo que parecen ser oportunidades para invertir.
- Evite los argumentos de venta agresivos para "invertir ahora".
- Ten cuidado con los respaldos de celebridades. Investiga en lugar de dejarte llevar por un cuentagotas de nombres.
- Si alguien afirma conocer una "mejor manera" de invertir, no confíes en él.



ACERCA DE LA DIVISIÓN FDACS DE SERVICIOS AL CONSUMIDOR

FDACS es la agencia estatal de protección al consumidor de Florida responsable de manejar las quejas de los consumidores y regular muchas industrias que afectan directamente a los consumidores de Florida. FDACS maneja más de 400,000 quejas y consultas de los consumidores, supervisa más de 500,000 dispositivos regulados, entidades y productos como bombas de gas y básculas de comestibles, realiza más de \$30,000 análisis de laboratorio en productos como gasolina y fluido de freno, realiza casi 9,000 inspecciones de paseo justo y devuelve más de \$2.8 millones a los consumidores a través de mediaciones con empresas.



La División de Seguridad Alimentaria supervisa los alimentos desde el punto de fabricación y distribución a través de las ventas al por mayor y al por menor para garantizar al público productos alimenticios seguros, saludables y debidamente representados.

OPRIMA EN EL ICONO ANTERIOR PARA VER LO RETIRADO, LOS RETIROS DEL MERCADO Y LAS ALERTAS DE SEGURIDAD



La Comisión de Seguridad de Productos de Consumo proporciona información sobre la retirada de productos de consumo como parte de la misión de la agencia de proteger a los consumidores y a las familias de los productos peligrosos.

OPRIMA EN EL ICONO ANTERIOR PARA VER LO RETIRADO, LOS RETIROS DEL MERCADO Y LAS ALERTAS DE SEGURIDAD.

El Departamento de Agricultura y Servicios al Consumidor de Florida es el centro de intercambio de información del estado para quejas, protección e información de los consumidores. Los consumidores que deseen información sobre la presentación de una queja contra una empresa o que crean que se ha producido fraude pueden visitarnos en línea en [FloridaConsumerHelp.com](https://www.floridaconsumerhelp.com) o ponerse en contacto con la línea directa de información y protección al consumidor del departamento llamando al 1-800-HELP-FLA (435-7352) o al 1-800-FL-AYUDA (352-9832) en español.