Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Guía de ciberseguridad para la pequeña empresa

Complejidad del material
SIMPLE ●○○

cyber.gov.au

Introducción

Para la pequeña empresa, incluso el incidente más pequeño de ciberseguridad puede tener un impacto devastador.
Esta guía tiene por objeto ayudar a las pequeñas empresas a protegerse de los incidentes de ciberseguridad más comunes. Como punto de partida recomendamos las tres medidas siguientes:

- Active la autenticación multifactorial
- Actualice su software
- Haga copias de seguridad de su información

Es posible que haya medidas en esta guía que no sean pertinentes a su empresa, o que su empresa tenga necesidades más complejas. Una vez que haya finalizado esta guía, recomendamos que las pequeñas empresas implementen el Nivel Uno de Madurez de los **Ocho esenciales**.
Si tiene preguntas sobre estos consejos o sobre la ciberseguridad en general, recomendamos que hable con un profesional de informática o un consejero de confianza.

Diríjase a cyber.gov.au para leer el texto completo de nuestra guía, que incluye consejos prácticos sobre cada medida.

Índice

Peligros para la pequeña empresa

Mensajes de estafa

Las estafas son una forma común en que los ciberdelincuentes atacan a las pequeñas empresas. Su objetivo es engañarle de modo que usted o su personal:

- envíen dinero o tarjetas de regalo
- hagan clic en enlaces o adjuntos maliciosos
- divulguen información confidencial, como contraseñas.

Los ciberdelincuentes suelen usar e-mails, mensajes de texto, llamadas telefónicas y medios sociales para intentar estafar a las empresas australianas. Suelen aparentar ser una persona u organización que usted piensa que es de confianza.

Ataques de mensajes fraudulentos

En particular, los **ataques de mensajes fraudulentos o phishing** son una preocupación para la pequeña empresa. Estas estafas suelen contener un enlace a un sitio web falso donde se alienta a la víctima a que se conecte a una cuenta o introduzca datos confidenciales.

Los ataques de mensajes fraudulentos generalmente ponen en peligro las contraseñas de cuentas. Los ciberdelincuentes suelen usar este método para «apropiarse» de las cuentas de medios sociales de las pequeñas empresas y exigir rescates.

Maneras de mitigar

Sea cauteloso si un mensaje proviene de una entidad conocida y parece sospechoso. Póngase en contacto con la persona o empresa por otro medio para comprobar si el mensaje es legítimo. Use los datos de contacto que encuentre en una fuente legítima; por ejemplo, visite el sitio web oficial de la empresa y no use los enlaces contenidos en el mensaje sospechoso.

Use los recursos siguientes para informarse más acerca de cómo identificar las estafas y los ataques de mensajes fraudulentos:

- Reconozca y denuncie las estafas
- Aprenda a detectar las estafas por mensaje fraudulento o phishing
- Cómo detectar los mensajes de ingeniería social.

Estudio de caso:

Una empleada de una compañía de mensajería recibió un e-mail de uno de los empleados ejecutivos que le pedía que compre 6 x tarjetas de crédito de MasterCard prepagas de $500. El ejecutivo le dijo que era algo confidencial pues las tarjetas serían vales de regalo para los empleados. Una vez compradas, se le pidió a la empleada que fotografiara ambas caras de las tarjetas y que se las enviara al ejecutivo como prueba de la compra.

Siguiendo las instrucciones, la empleada fue al correo y usó su tarjeta de crédito personal para comprar las tarjetas de regalo. Respondió al e-mail del ejecutivo y le envió fotos de las tarjetas de regalo como prueba.

Cuando regresó del correo, la empleada le entregó las tarjetas al ejecutivo, que no sabía nada de ellas. Un estudio de lo sucedido mostró que **todos los correos electrónicos sobre las tarjetas de regalo provenían de una dirección electrónica al azar y no de la cuenta de correo electrónico legítima del ejecutivo. Había sido una estafa.**

Los ataques por correo electrónico

Además de las estafas de tipo phishing, un ataque común a las pequeñas empresas es el **atentado al e-mail de la empresa** (BEC por sus siglas en inglés). Los delincuentes pueden hacerse pasar por representantes comerciales usando cuentas de correo electrónico interceptadas o por otros medios, como usar un nombre de dominio que parece similar a una empresa real. Aparte de robar información, estos ataques tienen generalmente por objeto estafar a las víctimas para que envíen fondos a una cuenta de banco administrada por el estafador.

Maneras de mitigar

La mejor defensa contra los ataques por e-mail es la capacitación y concientización de sus empleados. Asegúrese de que su personal sepa que siempre deben ser cautelosos ante los correos electrónicos que contienen:

- pedidos de pago, especialmente si son urgentes o vencidos
- cambios de los datos bancarios
- una dirección electrónica que no parece totalmente correcta, por ejemplo el nombre de dominio no coincide exactamente con el nombre de la compañía proveedora.

Si bien estos ataques pueden ser devastadores, las medidas de mitigación son fáciles y no cuestan casi nada. **Cuando el personal recibe e-mails así, la mitigación más eficaz es llamar al que lo envió para confirmar que el mensaje es legítimo.** No use datos de contacto que le hayan enviado pues podrían ser fraudulentos. Introduzca un proceso oficial que el personal debe seguir cuando recibe pedidos de pago o cuando cambian los datos bancarios.

Aprenda a proteger su empresa de las estafas por atentado al e-mail de la empresa y de intercepción del e-mail mediante los recursos siguientes:

- Atentado al e-mail de la empresa
- Proteja a su empresa del fraude por e-mail y de la intercepción del e-mail
- Qué hacer si su empresa ha sido víctima de fraude por e-mail o intercepción de e-mails.

Estudio de caso:

Una pequeña compañía de construcción recibió un e-mail de su proveedor en que le informaba que había cambiado de banco. El proveedor proporcionaba los datos nuevos de la cuenta para el pago de las facturas. Como el e-mail parecía genuino, **la empresa de construcción no llamó al proveedor para confirmar el cambio de los datos bancarios.**

La empresa pagó una factura del proveedor de más de $70.000. Al día siguiente, otro empleado pagó la misma factura nuevamente por error por un monto adicional de $70.000. En total se pagaron más de $150.000 a la nueva cuenta de banco.

Cuando la empresa llamó a su proveedor para pedirle que rembolsara el doble pago, el proveedor le informó que esos datos bancarios eran incorrectos. Se lanzó una investigación de inmediato y el proveedor descubrió que una de sus cuentas de correo electrónico había sido pirateada y estaba enviando datos bancarios fraudulentos. **No se recuperó dinero alguno.**

Software malicioso

Malware es un término general que abarca software malicioso como ransomware, virus, software espía o spyware y troyanos. El malware puede:

- robar o trabar el acceso a los archivos de su dispositivo
- robar los números de cuentas bancarias o tarjetas de crédito
- robar sus nombres de usuario y contraseñas
- tomar control de su computadora o espiar en ella.

El malware puede impedir el funcionamiento correcto de su dispositivo, suprimir o corromper sus archivos o darle acceso a personas ajenas a su información personal o comercial. Si su dispositivo está infectado con malware es posible que lo torne vulnerable a otros ataques. Además, el malware podría propagarse a otros dispositivos en la misma red.

Su dispositivo puede infectarse con malware de varias maneras, por ejemplo:

- visitar sitios web que están infectados con malware
- descargar de internet archivos o software infectados
- abrir archivos adjuntos a e-mails que están infectados.

Ransomware

El ransomware es un tipo de software malicioso común y peligroso. Funciona trabando o codificando sus archivos de modo que ya no tenga acceso a ellos. Se exige un rescate, generalmente pagado en criptomoneda, para restablecer el acceso a los archivos. Los ciberdelincuentes podrían también amenazar con publicar o vender datos en línea a menos que se les pague un rescate.

Maneras de mitigar

Si bien el software antivirus o de seguridad puede proteger del software malicioso, no hay software que sea eficaz al 100%. El personal debe mantenerse alerta a los e-mails, sitios web y descargas de archivos, y actualizar regularmente sus dispositivos para mantenerlos seguros.

Vea los recursos siguientes para obtener más información sobre la protección de su empresa contra el ransomware:

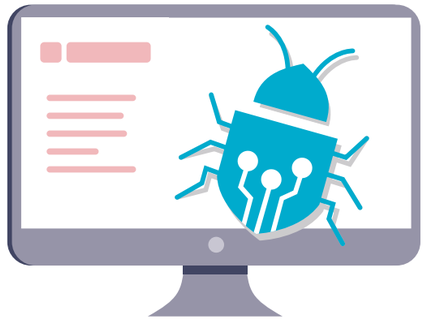
- Ransomware
- Protéjase de los ataques de ransomware
- Qué hacer si le exigen un rescate.

Estudio de caso:

Cuando los empleados de una tienda de repuestos para autos llegaron al trabajo una mañana no pudieron encender su servidor. Cuando el proveedor de TI consiguió acceder al servidor, encontró una ventana abierta que decía que se habían codificado todos los datos de la computadora. La nota exigía el pago de un rescate en bitcoins para destrabar los archivos.

La computadora estaba conectada a una unidad de copias de seguridad y ésta también había sido codificada. Intentaron conectar más unidades de copias de seguridad, pero los archivos se codificaban automáticamente en unos pocos segundos. **No habían suprimido el ransomware antes de intentar la recuperación de sus datos, y así perdieron todos los archivos de las copias de seguridad que tenían.**

La única opción que les quedaba era reconfigurar el servidor de fábrica y comenzar de cero con un sistema nuevo. La empresa perdió muchos años de datos y tuvo que comenzar desde el principio.



Proteja sus cuentas

Active la autenticación multifactorial

Cuando se utiliza la autenticación multifactorial (MFA por sus siglas en inglés) los ciberdelincuentes tienen más dificultades para conseguir acceso a sus cuentas.

La autenticación multifactorial añade otra capa de seguridad a su cuenta. Es una de las formas más eficaces de proteger sus cuentas del acceso no autorizado, de modo que debería usarla cuando sea posible. Quienquiera se conecte a su cuenta tendrá que proporcionar otra cosa además de su nombre de usuario y contraseña. Podría ser un código único de un mensaje de texto o aplicación de autenticación. Para obtener más información lea nuestros consejos sobre la MFA, disponibles en **cyber.gov.au/mfa**.

✓ **Active la MFA cuando sea posible, comenzando por sus cuentas más importantes.**

Implemente los controles de acceso

La restricción del acceso de los usuarios puede limitar el daño causado por los incidentes de ciberseguridad.

El control del acceso es una manera de limitar el acceso a determinados archivos y sistemas. Normalmente, el personal no necesita acceso a todos los datos, cuentas y sistemas de la empresa. Debería permitírseles el acceso solamente a lo que necesitan para hacer su trabajo.

La restricción del acceso limita el daño causado por los incidentes de ciberseguridad. Por ejemplo, si la computadora de un empleado se ve infectada por ransomware, con los controles de acceso apropiados podría afectar solamente un pequeño número de archivos, y no a toda la empresa.

✓ **Asegúrese de que cada usuario tenga acceso únicamente a lo que necesita para realizar su trabajo.**

Use contraseñas resistentes o frases de contraseña

Proteja sus cuentas de los ciberdelincuentes con una contraseña segura o frase de contraseña.

Muchas pequeñas empresas afrontan ataques cibernéticos porque tienen malas prácticas de contraseña. Por ejemplo, usan la misma contraseña para varias cuentas. Puede usar tanto un gerente de contraseñas como frases de contraseña para crear contraseñas resistentes.

Los **gerentes de contraseña** son como una caja fuerte virtual donde se guardan sus contraseñas. Se los puede usar para crear y guardar contraseñas resistentes y **únicas** para cada una de sus cuentas. Si tiene muchas cuentas, esto alivia la carga de recordar contraseñas únicas. No es necesario recordar las contraseñas o las cuentas a las que corresponden ya que está todo registrado en el gerente de contraseñas.

Si tiene cuentas a las que se conecta regularmente o que no quiere guardar en un gerente de contraseñas, piense en usar una frase de contraseña. Las frases de contraseña son una combinación de palabras al azar, por ejemplo «cristal cebolla arcilla rosquita». Son útiles cuando se necesita una contraseña segura que sea fácil de recordar. Use una mezcla al azar de cuatro o más palabras y que sea única, es decir **no vuelva a usar una frase de contraseña** para varias cuentas. Para obtener más información lea nuestros consejos sobre frases de contraseña y gerentes de contraseña que encontrará en **cyber.gov.au/passphrases**.

✓ **Use un gerente de contraseñas para crear y guardar contraseñas únicas para cada una de sus cuentas importantes.**

Gestión de las cuentas compartidas

Compartir cuentas puede poner en riesgo la seguridad, y causa dificultades para rastrear la actividad maliciosa.

En las pequeñas empresas puede haber razones legítimas por las que el personal tenga que compartir cuentas, pero esto debería evitarse lo más posible. Cuando varios empleados usan la misma cuenta puede resultar difícil rastrear la actividad para remontarse a un empleado determinado, y aún más difícil rastrear la entrada de ciberdelincuentes. A menos de cambiar la contraseña, los empleados también podrían seguir teniendo acceso a las cuentas después de haber dejado la empresa.

✓ **Limite el uso de cuentas compartidas y proteja las que se usan en su empresa.**

Proteja sus dispositivos e información

Actualice su software

Mantener el software al día es una de las mejores maneras de proteger su empresa de los ataques cibernéticos.

Las actualizaciones pueden corregir fallas de seguridad del sistema operativo y otro software de modo que el acceso les resulte más difícil a los ciberdelincuentes. Todo el tiempo se descubren nuevos defectos; por lo tanto, no ignore las instrucciones de poner el software al día. La actualización periódica del software reduce la posibilidad de que un ciberdelincuente utilice una debilidad conocida para ejecutar malware o piratear su dispositivo. Si necesita ayuda, el ACSC ha publicado orientación sobre las actualizaciones.

Si su dispositivo o software es demasiado viejo puede que no haya actualizaciones disponibles. Si el fabricante ha dejado de prestar apoyo al producto mediante actualizaciones, considere la posibilidad de modernizar y adquirir un producto más reciente para mantenerlo seguro. Ejemplos de sistemas que ya no reciben actualizaciones importantes: **iPhone 7** y **Microsoft Windows 7**.

Para obtener más información lea nuestra orientación sobre actualizaciones, disponible en **cyber.gov.au/updates**.

✓ **Active las actualizaciones automáticas de sus dispositivos y software.**

Use software de seguridad

El software de seguridad, como los antivirus y protección contra el ransomware, puede ayudar a proteger sus dispositivos.

Use software de seguridad para detectar y eliminar el malware de sus dispositivos. El software antivirus se puede configurar para que haga un estudio periódico en busca de archivos y programas sospechosos. Si encuentra un peligro, se recibe una alerta y el archivo sospechoso se pone en cuarentena o elimina.

Muchas pequeñas empresas pueden **usar Windows Security** para protegerse de los virus y software malicioso. Windows Security viene incorporado en los dispositivos con Windows 10 y Windows 11, e incluye protección gratuita contra los virus y peligros. También se lo puede usar para activar las funciones de protección contra el ransomware del dispositivo.

Para informarse sobre productos alternativos y opciones, lea nuestros consejos sobre el software antivirus: busque *antivirus* en cyber.gov.au.

✓ **Configure el software de seguridad para que realice barridos regulares en sus dispositivos.**

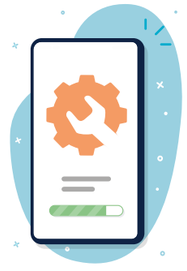
Haga copias de seguridad de su información

Las copias de seguridad regulares pueden ayudar a recuperar la información si se ha perdido o interceptado.

La preparación de copias de seguridad de la información importante debería ser una práctica regular o automática de su empresa. Sin ella, podría serle imposible recuperar su información después de un ataque cibernético.

Existen muchos métodos y productos que se pueden usar para hacer copias de seguridad de la información. Busque consejos detallados sobre las copias de seguridad de su empresa en consejos sobre copias de seguridad, en **cyber.gov.au/backups**. La mejor opción dependerá de cada empresa; por lo tanto, hable con un profesional de TI si no está seguro.

✓ **Cree e implemente un plan para hacer copias de seguridad de su información regularmente.**



Proteja sus servicios externos y de red

Proteja su empresa de los ataques cibernéticos: responda a eventuales vulnerabilidades de su red.

Los dispositivos y servicios de su red pueden ser un objetivo prioritario para los ciberdelincuentes. En muchos casos, puede resultar complejo proteger estos sistemas; por lo tanto, hable con un profesional de TI sobre las recomendaciones siguientes:

- **Proteja sus servidores**: Si usa un NAS u otro tipo de servidor en su casa o empresa, ponga atención extra en su protección. Estos dispositivos son objetivos comunes de los ciberdelincuentes porque suelen contener archivos importantes o desempeñar funciones importantes. La protección de estos dispositivos exige muchas estrategias de mitigación. Por ejemplo, es importante asegurarse de que los servidores o dispositivos NAS se actualicen regularmente. Las cuentas administrativas deberían estar protegidas con una frase de contraseña resistente o con autenticación multifactorial.
- **Minimice la huella visible externamente**: Haga auditorías y proteja todo dispositivo de su red expuesto a la internet. Esto podría incluir Remote Desktop, File Shares, Webmail y servicios de administración a distancia.
- **Migre a servicios en la nube:** Piense en usar servicios en línea o en la nube que ofrezcan seguridad incorporada en lugar de gestionar la propia. Por ejemplo, use servicios en línea para cosas como correo electrónico o alojamiento web en lugar de administrar y proteger esos servicios usted mismo.
- **Mejore la seguridad de su enrutador:** Siga nuestros consejos sobre maneras de proteger su enrutador, lo que incluye actualizar las contraseñas por defecto, activar un wifi específico para clientes e invitados y usar los protocolos de codificación más resistentes. Busque *router* en **cyber.gov.au** para obtener más información.
- **Comprenda su cadena de suministro cibernética:** Las empresas modernas suelen subcontratar muchos servicios. Por ejemplo, usan un proveedor de servicios gestionados para mantener su TI. Los problemas de seguridad de dichos servicios o proveedores podrían tener consecuencias significativas para su empresa. Para obtener consejos detallados sobre la gestión del riesgo de las cadenas de suministro cibernéticas, lea nuestra Orientación sobre las cadenas de suministro cibernéticas en **cyber.gov.au**.

✓ **Hable con un profesional de TI sobre las maneras de proteger su red.**

Aumente la resistencia de su sitio web

Los sitios web son un objetivo prioritario para los ataques cibernéticos.

Proteja su sitio web de la piratería mediante las siguientes medidas básicas de seguridad:

- proteja la conexión a su sitio web con autenticación multifactorial o una contraseña resistente
- actualice regularmente los sistemas de gestión de contenido y complementos (plugins) de su sitio web
- haga copias de seguridad de su sitio web regularmente de modo que pueda restablecerlo después de un ataque cibernético.

El ACSC tiene recursos adicionales a disposición de los propietarios de sitios web. Busque estos recursos en **cyber.gov.au**:

- Triunfos rápidos para su sitio web
- Implementación de Certificados, TLS, HTTPS y TLS oportunista
- Seguridad del sistema de nombres de dominio para los propietarios de dominio
- Preparación y respuesta ante los ataques de denegación de servicio

✓ **Lea sobre los recursos del ACSC sobre seguridad de sitios web.**

Reconfigure sus dispositivos antes de venderlos o disponer de ellos

Los datos contenidos en sus viejos dispositivos pueden ser accesibles a extraños.

Si no dispusiera de sus dispositivos de forma segura, ciberdelincuentes podrían acceder a la información que contienen. Esto incluye e-mails, archivos y otros datos comerciales. Elimine toda la información de sus dispositivos comerciales antes de venderlos, intercambiarlos o arrojarlos a la basura. Por ejemplo, mediante una reinicialización de fábrica. Con esto se borrará toda información y el dispositivo volverá a las configuraciones originales.

Para obtener consejos sobre la reinicialización de sus dispositivos, lea nuestros consejos en cómo disponer de su dispositivo de forma segura. Busque *disponer* en **cyber.gov.au**.

✓ **Realice una reinicialización de fábrica antes de vender o disponer de sus dispositivos comerciales.**

Mantenga sus dispositivos trabados y físicamente seguros

Restrinja el acceso a sus dispositivos comerciales para reducir las oportunidades de actividad maliciosa.

Limitar el acceso físico a los dispositivos de su empresa es una manera sencilla de impedir el robo de datos u otras actividades maliciosas. No tenga los dispositivos comerciales en sitios en los que el personal no autorizado o el público podrían acceder a ellos.

Use controles de seguridad para proteger aún más sus dispositivos comerciales. Como mínimo, trábelos con una frase de contraseña, PIN o biometría. Asegúrese de que estos dispositivos se traben automáticamente después de un corto período de inactividad.

✓ **Configure los dispositivos para que se traben automáticamente después de un corto tiempo de inactividad.**

Proteja los datos de su empresa

Los datos que guarda su empresa son un objetivo atractivo para los ciberdelincuentes.

Las brechas de datos están aumentando: no permita que su empresa sea una víctima más. Es importante comprender los datos que guarda su empresa, y en qué sitios. Una vez que lo sepa, use las recomendaciones de esta guía para proteger sus datos contra el acceso por ciberdelincuentes. La legislación también puede imponer obligaciones adicionales a algunas pequeñas empresas.

- **Consolide los datos de su empresa.** Es posible que tenga datos guardados en numerosos dispositivos o servicios. Cuando los datos están descentralizados aumenta el número de sistemas que debemos proteger y de los que tenemos que hacer copias de seguridad. Numerosos sistemas también pueden crear más oportunidades para ataques de ciberdelincuentes. Cuando sea posible, guarde los datos de su empresa en un sitio central que esté protegido y del que se hagan copias de seguridad regularmente. La centralización de sus datos puede crear una brecha más grande si los sistemas son vulnerados; por lo tanto, vele por la protección adecuada de este sitio central mediante configuraciones seguras y acceso restringido. Pida consejo a un profesional de TI o de ciberseguridad.

- **Conozca sus obligaciones de protección de datos.** Algunas pequeñas empresas pueden tener obligaciones jurídicas de gestión de la información personal que recaban. Obtenga más información en la guía para pequeñas empresas de la Oficina del Comisario de información de Australia, que encontrará en **oaic.gov.au**. Si tuviera dudas, consulte a un abogado.

✓ **Comprenda los datos que guarda su empresa y sus responsabilidades de protegerlos.**

Prepare a su personal

Instruya a su personal

Los empleados con buenas prácticas de ciberseguridad son la primera línea de defensa contra los ataques cibernéticos.

Sus empleados deberían ser conscientes de la ciberseguridad, lo que incluye los aspectos siguientes:

- amenazas de ciberseguridad comunes, como la vulneración del e-mail de la empresa y el ransomware
- medidas de protección, incluidas las contraseñas resistentes o frases de contraseña, la autenticación multifactorial o MFA y las actualizaciones del software
- cómo detectar estafas y ataques de phishing
- normativas específicas de la empresa (por ejemplo, los procesos para denunciar e-mails sospechosos o para confirmar que las facturas son auténticas antes de pagarlas)
- qué hacer en una emergencia.

El sitio web del ACSC tiene recursos sobre la mayoría de estos temas en cyber.gov.au/learn. Podría pensar en otras maneras de educar a sus empleados, por ejemplo, con un curso formal o capacitación interna. Cualquiera sea su decisión, recuerde que la capacitación sobre ciberseguridad no es un requisito de una sola vez, sino que se necesita actualización periódica.

✓ **Determine de qué manera se enseñará la concientización sobre ciberseguridad en su empresa.**

Formule un plan para emergencias

Un plan para emergencias podría reducir las consecuencias de un ataque cibernético para su empresa.

Cuando respondemos a un incidente de ciberseguridad, cada minuto cuenta. Tener un plan para emergencias implica que su personal pasará menos tiempo decidiendo qué hacer y más tiempo reaccionando.

Considere las preguntas siguientes al momento de formular su plan para emergencias:

- ¿Qué procedimiento sigue su personal para denunciar posibles incidentes de ciberseguridad?
- ¿Con quién se pone en contacto para pedir ayuda? Por ejemplo, profesionales de TI y su banco.
- ¿Cómo se informará del incidente al personal, los interesados o clientes?
- ¿Cómo se manejará la empresa si los sistemas críticos no están en línea?

Cerciórese de que su personal conozca bien el plan para emergencias, incluso sus funciones o responsabilidades, de tenerlas. Tenga una copia impresa del plan en caso de que sus sistemas estén fuera de línea cuando lo necesite.

✓ **Formule un plan para emergencias para los incidentes de ciberseguridad.**

Manténgase informado

Asóciese al ACSC para recibir las últimas noticias del ACSC.

Manténgase informado de los peligros y vulnerabilidades cibernéticas más recientes: asóciese al ACSC. Este servicio le enviará boletines mensuales y alertas cuando se identifique un nuevo peligro cibernético.

La ciberseguridad es un campo en evolución acelerada. Los ciberdelincuentes buscan y explotan las vulnerabilidades a los minutos de descubrirlas. Manténgase informado sobre el panorama de ciberseguridad para ayudar a su empresa a comprender los peligros que probablemente enfrente y cómo protegerse de ellos.

✓ **Inscriba su empresa en el Programa de socios de ACSC.**

Descargo de responsabilidad

El material contenido en esta guía es de naturaleza general y no debe considerarse asesoramiento jurídico ni utilizarse para ayudar en una situación en particular o en una emergencia. En todo asunto importante, se aconseja obtener asesoramiento profesional independiente apropiado a su situación.

La Commonwealth no acepta responsabilidad alguna por daños, pérdidas o gastos incurridos por haber dependido de la información contenida en esta guía.

Para obtener más información o denunciar un incidente de ciberseguridad, póngase en contacto con nosotros:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Este número es para llamadas en Australia únicamente.

Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre