

# SUGERENCIAS DE CIBERSEGURIDAD

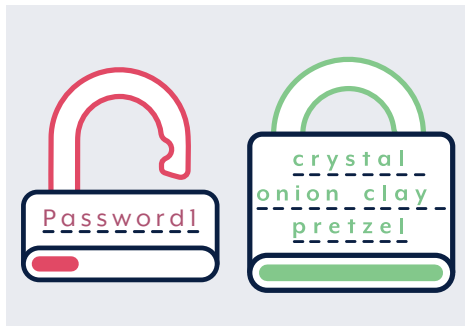
## MÉTODOS PRÁCTICOS PARA PROTEGERSE EN LÍNEA

[cyber.gov.au/learn](https://cyber.gov.au/learn)



### Actualice sus aplicaciones y dispositivos

La actualización de los dispositivos puede resolver problemas y responder a nuevas inquietudes de seguridad o debilidades que los hackers podrían usar para acceder a sus dispositivos o cuentas. También pueden agregar nuevas funciones.



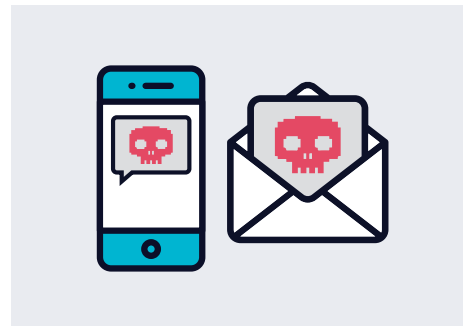
### Configure frases de contraseña seguras

Cuando no fuera posible usar la autenticación multifactorial (MFA), use una frase de contraseña para proteger su cuenta. Las frases de contraseña son contraseñas resistentes que usan un mínimo de cuatro palabras al azar. Los ciberdelincuentes tienen dificultades en adivinarlas, pero usted las recordará fácilmente.



### Active la autenticación multifactorial (MFA)

La autenticación multifactorial significa que tenemos instalado más de un control para demostrar la identidad en la cuenta. Por ejemplo, puede que necesite un código enviado por mensaje de texto y su frase de contraseña. Así, los ciberdelincuentes tienen más dificultades para conseguir acceso a nuestras cuentas.



### Reconozca y denuncie las estafas

Los delincuentes suelen usar e-mail, SMS, llamadas telefónicas y los medios sociales para estafar a la gente. Generalmente se ponen en contacto con usted, y fingen ser una persona u organización que usted conoce y que es de confianza.

Manténgase siempre alerta cuando haga clic en archivos adjuntos o enlaces que vienen en e-mails o mensajes.



### Establezca y realice copias de seguridad regularmente

La copia de seguridad es una copia digital de su información más importante en un dispositivo de almacenamiento externo o en un servidor en internet, como la nube. Significa que podrá restablecer sus archivos si hay un problema.



### Aumente el nivel de su ciberseguridad...

- Piense en lo que está publicando.
- Reciba alertas sobre nuevos peligros. Suscríbese a nuestro servicio de alerta gratis.
- Converse sobre la ciberseguridad con sus familiares y amigos.
- Evite el Wifi público cuando se conecte con su banco o haga compras en línea.
- Denuncie los ataques e incidentes cibernéticos para mantener la seguridad de Australia.

Más información [cyber.gov.au/learn](https://cyber.gov.au/learn)

**Denuncie los incidentes de ciberseguridad:**  
[cyber.gov.au](https://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