

Prevención de pérdida o robo de equipos o datos

La pérdida física de su equipo (o de los datos a los que tiene acceso y con los que trabaja a diario) debe protegerse con cautela. Lo más importante que debe saber es lo siguiente:

Tan pronto como se percate de que alguien pudo haber robado su dispositivo o equipo, o de que este se extravió, notifique a su supervisor y al profesional de seguridad de TI de inmediato para que se puedan tomar las medidas adecuadas para proteger los datos guardados en dicho dispositivo o equipo.

Los datos guardados ahora están comprometidos y son susceptibles de acceso, difusión y uso no autorizados. Se trata de una infracción cibernética grave que debe gestionarse por profesionales de seguridad de TI capacitados.

Acción: informar

Póngase en contacto con su administrador de TI, gerente de la clínica o supervisor inmediato.

¿Hay alguna actividad sospechosa en su sistema? Añada el nombre y número a esta hoja como referencia.

**Es imprescindible que la acción sea rápida.
¡Esta amenaza es real!**



Pasos a seguir

Repase esta lista de mejores prácticas y siga cada recomendación.

Consejos para proteger el equipo y evitar la pérdida de datos:

- Nunca** deje su computadora portátil o iPad sin supervisión en el trabajo o durante su traslado.
- Siga la política de contraseñas y actualice las contraseñas según sea necesario.
- Nunca** comparta su contraseña con nadie.
- Siga la política de la empresa sobre el acceso a sitios en internet.
- Evite utilizar unidades USB en la computadora de su organización.
- Cifre los datos confidenciales.
- Informe de inmediato cualquier pérdida de equipo o actividad sospechosa en su sistema.
- Avise sin demora a los funcionarios adecuados si algo parece sospechoso.
- Mantenga su lista de contactos de emergencia cerca.

Las medidas proactivas contribuyen en gran medida a protegerlo a usted y a los datos que gestiona.

Informar

Informar a:

Información
de contacto:

Para obtener más recursos e información sobre cómo puede proteger a sus pacientes de las amenazas cibernéticas, consulte la publicación *Prácticas de ciberseguridad de la industria de la salud (Health Industry Cybersecurity Practices, HICP): gestión de amenazas y protección de pacientes* en [405d.hhs.gov](https://www.hhs.gov/405d).