

Decálogo de Ciberseguridad

Yo protejo mis datos

Tip 1

¡Protege tus contraseñas!

Cuida que tus contraseñas sean secretas y robustas.

Cámbialas periódicamente.

No debes anotarlas ni compartirlas.



Tip 2

¡Alertas de seguridad!

Siempre que esté disponible activa la verificación en dos pasos y los avisos de inicio de sesión sospechosos.



Tip 3

¡Navega en páginas web seguras!

Comprueba la seguridad de los sitios que visitas, a la izquierda de la dirección web, busca el estado de seguridad:

-  Seguro
-  Información o no seguro
-  No seguro o peligroso



Tip 4

¡Realiza copias de seguridad!

Protege la información guardada en tu equipo y realiza copias de seguridad periódicas.



Tip 5

¡Protege tu información!

No transportes información sensible en dispositivos extraíbles.

Compártela en Google drive correctamente.

Procura eliminar de forma segura cualquier medio que contenga tu información.



Tip 6

¡Bloquea o finaliza sesión en los equipos!

Siempre que hayas concluido tus actividades bloquea la sesión de tu equipo y cierra las sesiones en todas las aplicaciones cuando trabajes en un equipo ajeno.



Tip 7

¡Ten cuidado con las conexiones wifi externas!

Evita utilizar redes inalámbricas externas o públicas al manejar información sensible.



Tip 8

¡Protege los equipos UPAEP!

No descargues ni instales software o aplicaciones no autorizadas por la misma Universidad en equipos propiedad de UPAEP.

Si tienes necesidades específicas comunícate al #911 y pide asesoría con los especialistas.

Revisa el software estándar instalado en los equipos UPAEP en upaep.mx/cau



Tip 9

¡Mantente actualizado!

Mantén actualizado tu equipo y todas las aplicaciones.



Tip 10

¡Mantente informado!

Presta atención a los avisos de seguridad publicados en medios institucionales.

Ante cualquier actividad sospechosa o anómala, comunícate al #228 o entra a upaep.mx/cau



#UPAEPContigo

Mayores informes:
Centro de Atención al Usuario
cau@upaep.mx