



Seguridad Digital: Protege tu Cuenta

Todo lo que necesitas saber para mantener tu cuenta universitaria segura.



¿Por qué importa la seguridad?

Información valiosa

Tu cuenta universitaria contiene datos personales y académicos que debes proteger.

Amenaza real

Los ciberataques en universidades son cada vez más frecuentes y sofisticados.

Responsabilidad de todos

Proteger la red institucional empieza con las decisiones de cada estudiante.



Piensa Antes de Hacer Clic

No todo lo que llega a tu correo es real. Los atacantes son expertos en crear mensajes convincentes.

- **Verifica el remitente** – ¿el nombre coincide con el dominio del correo?
- **Revisa el enlace** – pasa el cursor sobre él antes de hacer clic.
- **Desconfía si piden datos sensibles** – ninguna institución legítima los solicita por correo.

Señales de Alerta: Identifica el Phishing

Urgencia falsa

"Tu cuenta será bloqueada hoy" –
Los atacantes usan el miedo para
apresurarte a actuar sin pensar.

Enlaces sospechosos

El texto del enlace dice una cosa,
pero el dominio al que apunta es
completamente diferente.

Solicitudes extrañas

Te piden contraseña, código MFA
o datos personales por correo o
formulario desconocido.

 Si algo te parece raro, probablemente lo es. Ante la duda, no hagas clic.

Crea una Contraseña Fuerte

Tu contraseña es la primera línea de defensa. Hazla difícil de adivinar y fácil de recordar solo para ti.



Mínimo 12 caracteres

Combina mayúsculas, minúsculas, números y símbolos.



Evita lo obvio

Nada de RUT, nombre, fecha de nacimiento ni "123456".



Una contraseña por servicio

Si una cuenta es comprometida, las demás permanecen seguras.

MFA: Tu Segunda Barrera de Seguridad



La **Autenticación Multifactor (MFA)** combina tu contraseña con un código único generado en tu teléfono.

Contraseña robada

Aunque alguien consiga tu contraseña, no puede acceder sin el código de tu teléfono.

Código en tu teléfono

Solo tú tienes acceso al dispositivo que genera o aprueba el código de ingreso.

Solicitud no iniciada

Si recibes una solicitud MFA que tú no pediste, **recházala de inmediato.**

Instala Microsoft Authenticator



Sigue estos 4 pasos:



Abre Google Play o App Store



Busca "Microsoft Authenticator"

Verifica que sea de **Microsoft Corporation**.



Instala y abre la app



Permite las notificaciones

Vincular tu cuenta con Authenticator



Computador

Inicia sesión con tu cuenta institucional



Microsoft

Cuando solicite configurar seguridad,
elige Authenticator



Teléfono

Authenticator → + → Cuenta
profesional o educativa



Código QR

Elige "Escanear código QR" y apunta al
QR del computador



Prueba

Aprueba la notificación para terminar

 Mantén el código QR abierto en el computador hasta completar el registro.

4 Reglas para Recordar



Piensa

Antes de hacer clic en enlaces o descargar archivos, verifica su origen.



Protege

Usa contraseñas fuertes, únicas y de al menos 12 caracteres para cada servicio.



Activa

Configura MFA con Microsoft Authenticator en tu cuenta institucional.



Rechaza

Cualquier solicitud de acceso o código que tú no hayas iniciado.



Recuerda: la seguridad digital es un hábito, no una tarea de una sola vez.