¡Tu mejor aliado
eres tú!
Ahorrando para tu futuro

GUÍA DE **CIBERSEGURIDAD** PARA TODOS

Protege tu información en el mundo digital

EN ESTA GUÍA APRENDERÁS SOBRE:

- Ataques de Phishing
- Contraseñas Seguras
- Autenticación Multifactor (MFA)
- Detección de Sitios No Confiables

Tu seguridad es nuestra prioridad

RECOMENDACIONES FINALES

Hábitos para mantenerte protegido

Mantén todo actualizado
Mantén siempre actualizado tu sistema operativo, navegador y aplicaciones, ya que las actualizaciones corrigen fallas de seguridad.

Desconfía de enlaces sospechosos
No hagas clic en enlaces ni descargues archivos adjuntos no solicitados, incluso si parecen venir de personas conocidas.

Verifica directamente
Cuando tengas dudas sobre un correo de tu banco u otra empresa, no hagas clic en los enlaces. Mejor escribe la dirección oficial directamente en tu navegador o llama al número que aparece en el reverso de tu tarjeta.

Haz copias de seguridad
Realiza copias de seguridad de tu información importante en discos externos o servicios en la nube confiables.

Revisa tus cuentas
Revisa periódicamente los movimientos de tus cuentas bancarias y notificaciones de inicio de sesión en tus servicios.

RECUERDA

En ciberseguridad, la mejor defensa es la duda saludable. Si algo te parece extraño, **urgente** o demasiado **bueno** para ser verdad, probablemente lo sea. Tómate un momento para verificar antes de **actuar.**

AFP ATLÁNTIDA
CANALES DE SERVICIO

Contact Center:
2280-3000

Correo:
afp@afpatlantida.com

Sitio web:
www.afpatlantida.com

DETECTAR SITIOS **NO CONFIABLES**

Antes de entregar tus datos, verifica

Antes de ingresar tus datos en cualquier página, revisa estas señales que te ayudarán a distinguir un sitio legítimo.

Lo que debe tener un sitio confiable

Candado en la barra de direcciones
Verás un pequeño candado al lado de la URL, indicando que la conexión es segura (HTTPS). Sin embargo, ojo: esto solo significa que la conexión está cifrada, no que el sitio sea legítimo.

Dirección web correcta
Verifica letra por letra. Los estafadores usan dominios muy parecidos:
arnazon.com en lugar de amazon.com
paypa1.com en lugar de paypal.com

Información de contacto clara
Empresas serias tienen dirección física, teléfono y correo de contacto verificable.

Diseño profesional
Aunque no es garantía, los sitios falsos suelen tener imágenes pixeladas, errores ortográficos o diseños desactualizados.

SEÑALES DE ALARMA

- Ofertas demasiado buenas para ser verdad ("iPhone nuevo a $50")
- Pagos por métodos no rastreables (transferencias directas, cripto)
- Ventanas emergentes dicen que tu computadora está infectada
- URLs muy largas y extrañas con muchos números y caracteres raros
- El sitio te redirige automáticamente a otras páginas
- Piden información que no es necesaria para la transacción
- No tienen políticas de privacidad ni términos y condiciones

Herramientas para verificar sitios

Google Safe Browsing:
transparencyreport.google.com/safe-browsing/search
VirusTotal: virustotal.com (analiza enlaces sospechosos)
WHOIS: Te dice cuándo se creó un dominio (los fraudulentos suelen ser muy nuevos)

ATAQUES DE PHISHING

El phishing es como cuando alguien se disfraza para engañarte. Los ciberdelincuentes se hacen pasar por bancos o personas conocidas para robarte información valiosa como contraseñas, números de tarjetas o datos personales.

Tipos de phishing más comunes

Phishing por correo electrónico
Es el más conocido. Recibes un correo que parece ser de tu banco diciendo que "tu cuenta será bloqueada" y te piden hacer clic en un enlace. Ese enlace te lleva a una página falsa que se ve idéntica a la real, pero al ingresar tus datos, los delincuentes los capturan.

Smishing (phishing por SMS)
Llegan mensajes de texto urgentes como "Tu paquete no pudo ser entregado, confirma tu dirección aquí" con un enlace sospechoso. También son comunes los mensajes que dicen que ganaste un premio.

Vishing (phishing por llamada telefónica)
Te llaman haciéndose pasar por empleados del banco, soporte técnico o incluso autoridades.

Spear phishing
Es un ataque dirigido específicamente a ti. El atacante investiga tu vida (redes sociales, trabajo, amigos) y crea un mensaje muy personalizado que parece totalmente real.

Phishing por redes sociales
Mensajes de "amigos" pidiendo dinero o vendiendo dolares, ofertas falsas en Facebook o Instagram.

SEÑALES DE ALERTA

- Mensajes con sentido de urgencia: "¡Actúa ahora o perderás tu cuenta!"
- Errores de ortografía o gramática extraños
- Saludos genéricos como "Estimado cliente" en lugar de tu nombre
- Direcciones de correo con pequeñas diferencias (ej: soporte@bancoo.com)

CONTRASEÑAS SEGURAS

Tu primera línea de defensa

Una contraseña débil es como dejar la puerta de tu casa con un candado de juguete. Veamos cómo crear contraseñas que realmente protejan tu información.

Características de una contraseña fuerte

- Al menos 12 caracteres
- Combina mayúsculas y minúsculas
- Incluye números
- Agrega símbolos especiales (@, #, $, %, &)

LO QUE NUNCA DEBES HACER

Usar la misma contraseña en varios sitios
Usar información personal: nombre o fecha de nacimiento
Contraseñas obvias como 123456, password, qwerty o admin
Compartir tus contraseñas por mensaje, correo o teléfono
Anotarlas en papeles visibles o archivos sin protección

SOLUCIÓN PRÁCTICA: **GESTORES DE CONTRASEÑAS**

Es imposible recordar contraseñas únicas para cada sitio. Por eso existen los gestores de contraseñas comoBitwarden, 1Password o Dashlane. Solo necesitas recordar una contraseña maestra y la aplicación se encarga del resto, generando y guardando contraseñas únicas y complejas para cada sitio.

AUTENTICACIÓN MULTIFACTOR (MFA)

Doble cerradura para tu seguridad

La MFA es como tener doble cerradura en tu puerta. Aunque alguien tenga tu contraseña, necesitará un segundo elemento para entrar.

¿Cómo funciona?
Cuando inicias sesión, además de tu contraseña, el sistema te pide una segunda verificación que puede ser:

- Un código que llega a tu celular por SMS o aplicación
- Una huella digital o reconocimiento facial
- Una llave física de seguridad (como una USB especial)
- Una notificación en tu teléfono que debes aprobar

Tipos de MFA: del más seguro al menos seguro

NIVEL	MÉTODO
MÁXIMA	Llaves físicas de seguridad (YubiKey, Google Titan) El método más seguro que existe.
ALTA	Aplicaciones autenticadoras (Google Authenticator, Microsoft) Generan códigos que cambian cada 30 segundos.
BUENA	Notificaciones push Recibes una alerta en tu app y solo apruebas o rechazas. Cómodas y seguras.
BÁSICA	SMS (mensaje de texto) Mejor que nada, pero el menos seguro: pueden interceptar mensajes mediante SIM swapping.

¿Dónde activar MFA?
Actívala en TODAS las cuentas importantes: Correo electrónico (¡prioridad número uno!), APPs de Banco y servicios financieros, Redes sociales, Servicios de pago como PayPal.

¿Por qué el correo es prioridad? Si hackean tu correo, pueden recuperar las contraseñas de todas tus demás cuentas.