Universidad de Caldas

OFICINA ASESORA DE PLANEACIÓN Y SISTEMAS

CIRCULAR N°1

Para: Estudiantes, docentes y personal administrativo de la Universidad de Caldas.

De: Grupo Interno de Sistemas

Asunto: Seguridad Informática / Protección contra amenazas en correo electrónico

Fecha: 24 de noviembre de 2025

⚠️ ALERTA: Incremento de ataques cibernéticos vía correo electrónico

Comunidad universitaria:

En los últimos meses hemos identificado un aumento significativo en los intentos de ataques cibernéticos a través del correo electrónico. Es fundamental que todos estemos alertas y sigamos las mejores prácticas de seguridad para proteger nuestra información institucional y personal.

⚠️ Principales Amenazas Informáticas

🎣 Phishing (Suplantación de Identidad)

Correos fraudulentos que imitan comunicaciones legítimas de bancos, instituciones o empresas conocidas para robar credenciales, información financiera o datos personales. Los atacantes crean páginas web falsas prácticamente idénticas a las originales.

🦠 Malware y Virus

Software malicioso oculto en archivos adjuntos (documentos, PDFs, ejecutables) que al abrirse infecta el equipo, permitiendo robo de información, espionaje o daño al sistema operativo y archivos.

ucaldas@ucaldas.edu.co www.ucaldas.edu.co PBX (57)(6) 878 15 00 Calle 65 # 26 - 10 | Manizales - Colombia

Universidad de Caldas

🔐 Ransomware

Tipo de malware que cifra todos los archivos del computador y de las unidades conectadas, exigiendo un pago (rescate) para recuperar el acceso. Puede propagarse por toda la red institucional.

🎭 Spoofing (Falsificación de remitente)

Correos que aparentan provenir de colegas, directivos o contactos conocidos, solicitando información confidencial, transferencias de dinero o cambios en procedimientos establecidos.

🔗 Enlaces Maliciosos

Links que redirigen a sitios web falsos o infectados que descargan automáticamente software malicioso, roban credenciales o recopilan información del navegador sin consentimiento.

🚨 Señales de Alerta - NUNCA ignore estos indicadores

- ⚠️ Solicitudes urgentes de información confidencial o cambios de contraseña
- ⚠️ Errores ortográficos o gramaticales inusuales en correos "oficiales"
- ⚠️ Direcciones de correo sospechosas o ligeramente diferentes a las conocidas
- ⚠️ Ofertas demasiado buenas para ser verdad o premios inesperados
- ⚠️ Amenazas o presión para actuar inmediatamente
- ⚠️ Archivos adjuntos inesperados, incluso de contactos conocidos
- ⚠️ Enlaces que al pasar el cursor muestran URLs diferentes al texto visible

✅ Recomendaciones de Seguridad

✓ Verificar el remitente

Revise cuidadosamente la dirección de correo completa del remitente, no solo el nombre mostrado. Ante cualquier duda, contacte al remitente por otro medio (teléfono, chat interno) para confirmar la autenticidad.

✓ No abrir archivos adjuntos sospechosos

Nunca abra archivos adjuntos de remitentes desconocidos o inesperados. Si recibe un archivo de un contacto conocido pero no lo esperaba, verifique con esa persona antes de abrirlo.

✓ Verificar enlaces antes de hacer clic

Pase el cursor sobre los enlaces sin hacer clic para ver la URL real. Si es sospechosa o no coincide con el destino esperado, no haga clic. Escriba manualmente la dirección en su navegador si necesita acceder al sitio.

ucaldas@ucaldas.edu.co www.ucaldas.edu.co PBX (57)(6) 878 15 00 Calle 65 # 26 - 10 | Manizales - Colombia

✓ Desconfiar de solicitudes urgentes

Los atacantes usan la urgencia como táctica. Ninguna institución legítima solicitará información confidencial, contraseñas o transferencias por correo electrónico de manera urgente o amenazante.

✓ Mantener software actualizado

Mantenga su sistema operativo, navegador, antivirus y aplicaciones siempre actualizadas. Las actualizaciones incluyen parches de seguridad críticos.

✓ Usar contraseñas fuertes y únicas

Utilice contraseñas diferentes para cada servicio, con mínimo 12 caracteres combinando mayúsculas, minúsculas, números y símbolos. Active la autenticación de dos factores cuando esté disponible.

✓ Reportar incidentes inmediatamente

Si sospecha haber sido víctima de un ataque, recibió un correo sospechoso o accidentalmente abrió un archivo malicioso, reporte de inmediato al área de TI para tomar medidas preventivas.

IMPORTANTE - Qué NO hacer NUNCA

- ⚠ Proporcionar contraseñas por correo electrónico o teléfono
- ⚠ Descargar archivos de fuentes no verificadas
- ⚠ Usar redes WiFi públicas sin VPN para acceder a información institucional
- ⚠ Compartir información confidencial sin verificar la identidad del solicitante
- ⚠ Ignorar advertencias de seguridad del navegador o antivirus
- ⚠ Conectar dispositivos USB desconocidos a equipos institucionales

La Seguridad es Responsabilidad de Todos

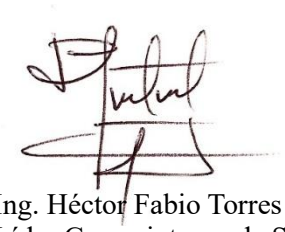
Su colaboración y vigilancia son fundamentales para mantener segura nuestra información institucional. Ante cualquier duda o sospecha, es mejor prevenir y consultar que lamentar un incidente de seguridad.

ucaldas@ucaldas.edu.co www.ucaldas.edu.co PBX (57)(6) 878 15 00 Calle 65 # 26 - 10 | Manizales - Colombia

Contacto Área de TI y Seguridad Informática

Mesa de ayuda: ayuda.ucaldas.edu.co/web

Cordialmente



Ing. Héctor Fabio Torres Martínez
Líder Grupo interno de Sistemas