ALCALDÍA DE
ACACÍAS

Capacitación en Ciberseguridad

protegiendo la información institucional y los datos de nuestra comunidad.

ING. Orley Minela Riveros

Oficina TIC

🔐 ¿Qué es la Ciberseguridad?

La ciberseguridad es el conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas, redes, programas y datos de ataques digitales, accesos no autorizados y daños.

🛡️ **Confidencialidad**

Solo personas autorizadas acceden a la información

✅ **Integridad**

Los datos no son alterados sin autorización

⚡ **Disponibilidad**

La información está accesible cuando se necesita.

⚠️ ¿Por qué es importante para nosotros?

Aumento de ciberataques a entidades públicas en Latinoamérica (2023) **+300%**

Costo promedio de una filtración de datos (IBM, 2023) **$4.45M (Dolares)**

📋 **Datos sensibles de ciudadanos**

Información personal, trámites, documentos oficiales

💰 **Recursos públicos**

Sistemas financieros y presupuestales

🏛️ **Confianza institucional**

Reputación y credibilidad ante la comunidad

ALCALDÍA DE ACACÍAS

Amenazas Comunes

Phishing

Correos o mensajes falsos que imitan ser de fuentes confiables para robar credenciales

Ransomware

Software malicioso que cifra archivos y exige pago para recuperarlos

Ingeniería Social

Manipulación psicológica para obtener información confidencial

Contraseñas Débiles

Uso de claves fáciles de adivinar o reutilizadas en múltiples cuentas

ALCALDÍA DE ACACÍAS

🎣 Cómo identificar un Phishing

❌ Señales de Alerta

- Remitente desconocido o sospechoso
- Urgencia extrema: "¡Actúe ahora!"
- Errores ortográficos y gramaticales
- Enlaces con URLs extrañas
- Solicitan datos personales o contraseñas
- Archivos adjuntos inesperados

✅ Qué Hacer

- Verificar el remitente cuidadosamente
- No hacer clic en enlaces sospechosos
- Contactar al remitente por otro medio
- Reportar a sistemas/TI inmediatamente
- No descargar archivos sospechosos
- Ante la duda, ¡no responder!

ALCALDÍA DE ACACÍAS

🎣 Cómo identificar un Phishing

https://www.apple.com

https://www.apple.com

ALCALDÍA DE ACACÍAS

Equipo Microsoft <irenebasto@hotmail.com>
Lun 15/03/2021 10:24 AM
Para: tecnicialsupp0rting@outlook.com

tu cuenta ha sido desactivada

Debido a cambios en la política de seguridad de Microsoft, desactivamos tu cuenta por no cumplir con el protocolo de nuevas credenciales. Para evitar la baja de nuestros servicios debe iniciar sesión en los servicios de Microsoft - Windows Live Outlook®, se le pedirá que especifique su dirección de correo electrónico y una contraseña, a las que nos referimos como sus credenciales de Microsoft - Windows Live Outlook®

Status: **Desactivada.**
Reason: **Renovar credencial**
Referencia de soporte: **PD2O266-VE332BL4**

Usted tiene **3** días a partir del envío de esta notificación, para renovar las credenciales de su cuenta de - Windows Live Outlook®, pasado ese tiempo **su cuenta quedará automáticamente eliminada**.

Para **Reactivar su cuenta** y usar su cuenta de Microsoft - Windows Live Outlook®, haga clic en **Renovar Credenciales**

Activar cuenta Windows Live Outlook®

Si desea eliminar su cuenta permanentemente, haga caso omiso a este correo.

Atentamente.
Windows Live Outlook®

Phishing y BEC: Fraude por Suplantación

Casos Críticos en un ente público

Ajuste de Nómina: Correos de remitentes externos solicitando descargas de archivos infectados.

Ataque BEC: Mensajes que simulan ser del Alcalde solicitando datos confidenciales por canales no oficiales.

Tip Pro: Siempre pase el puntero sobre el remitente. La dirección oficial DEBE ser **@acacias.gov.co.**

ALCALDÍA DE ACACÍAS

Malware Operativo

Software malicioso: Código hostil diseñado para infiltrarse, dañar archivos o tomar control de la red municipal.

Vectores de Riesgo Crítico

Gusanos (Worms)

Propagación automática. Infectan toda la Alcaldía en minutos a través de la red local.

Spyware

Keyloggers que capturan cada tecla para robar contraseñas de bancos y sistemas tributarios.

Troyanos

Disfraz de archivos legítimos (Resolución.pdf.exe) que abren accesos remotos ilegales.

Alerta de Seguridad Física

USB

Recomendación

No cargue su celular personal en los puertos USB de los computadores de la oficina.

RIESGO: Los cables de datos pueden transferir malware entre su dispositivo y la red institucional de forma invisible.

Ransomware:
Secuestro Digital

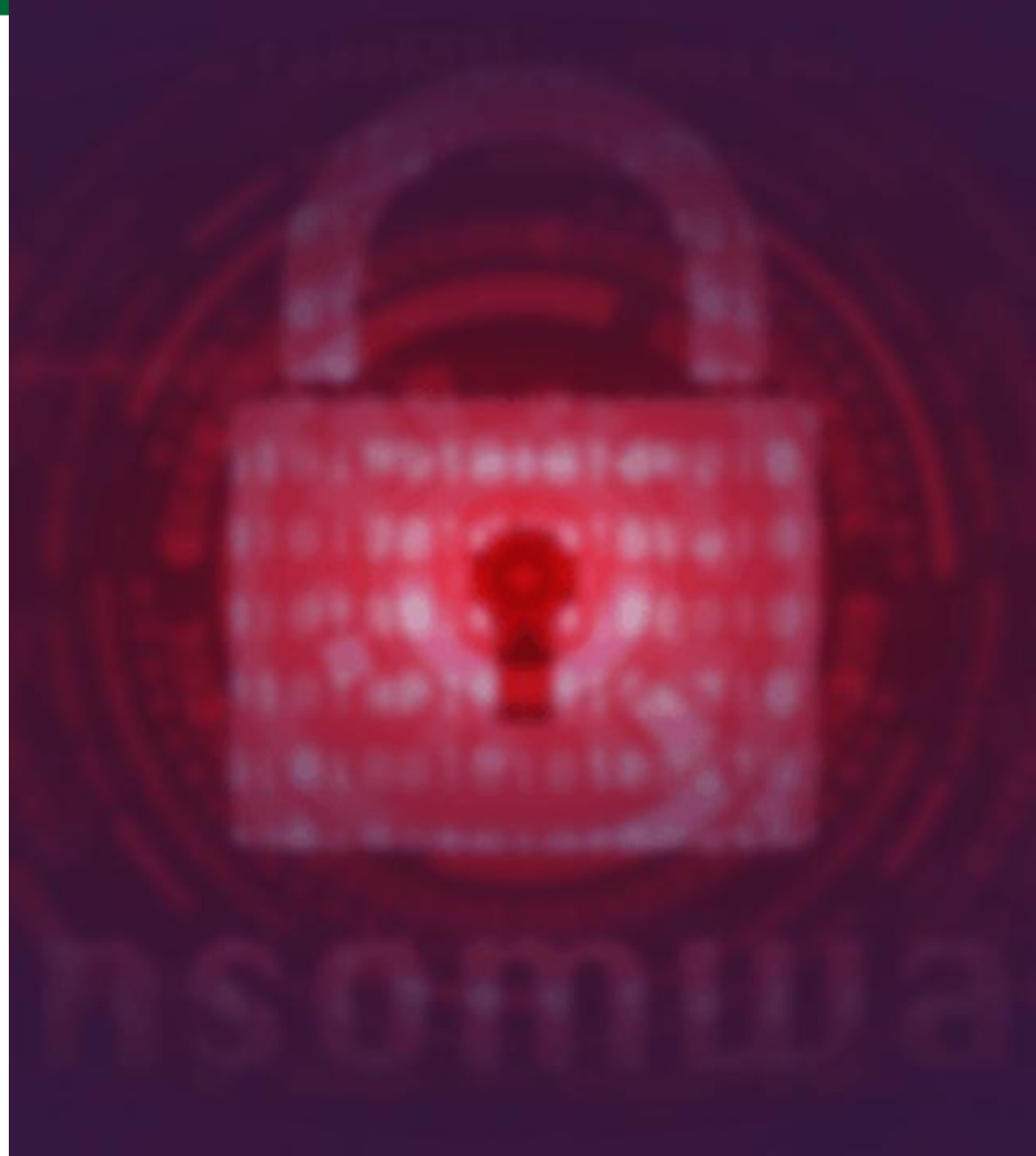
Impacto: Parálisis Total

El cifrado de archivos bloquea la atención ciudadana y destruye expedientes históricos.

Protocolo de Protección:

Use exclusivamente los **Discos de Red Institucionales (Drive)**.

Cuentan con copias de seguridad automáticas.



🔑 Contraseñas Seguras

Tip Una contraseña segura es tu primera línea de defensa

Características de una buena contraseña:

✓Mínimo 12 caracteres

✓Combina mayúsculas y minúsculas

✓Incluye números y símbolos

✓No usar información personal

✓Única para cada cuenta

Ejemplo de técnica:

Frase memorable:

"Mi café favorito cuesta 5 mil pesos"

Contraseña resultante:

McF@v0r1t0C$5mP!

⚠️ **Nunca compartas tu contraseña con nadie**

Protocolo de Escritorio Seguro

Win + L: Bloqueo inmediato al retirarse de su puesto, sin excepción.

Passphrases: Use frases largas (ej. Acacias-TierraDeP@z2026*) en lugar de claves cortas.

Cero Post-its: Prohibido pegar claves físicas en monitores o teclados.

ALCALDÍA DE ACACÍAS

Plan de Reacción ante Incidentes

1. AISLAR

Desconecte el cable de red o apague el Wi-Fi. **No apague el equipo** (preserva evidencia).

2. REPORTAR

Informe de inmediato a la **Oficina TIC** de la Alcaldía

3. ASEGURAR

Desde su celular, cambie claves de correo institucional y bancos de forma urgente.

ALCALDÍA DE ACACÍAS

"Cada clic abre una puerta a una oportunidad, pero también a un riesgo. La integridad de nuestros datos depende de la prevención activa."

EVALUACIÓN FINAL DE LA CAPACITACIÓN
19 DE FEBRERO DE 2026

ALCALDÍA DE ACACÍAS