



Pereira, 03 de diciembre de 2025

DE: CARLOS FERNANDO GARCIA CAICEDO - Director Operativo de Infraestructura Tecnológica  
- 410 Dirección de Infraestructura Tecnológica

PARA: Alcaldía de Pereira



No. 20251203-68565-I

ASUNTO: Citación a capacitación "Buenas Prácticas en Ciberseguridad"

Cordial saludo:

Por medio del presente, nos permitimos informar y citar a la capacitación titulada **"Buenas Prácticas en Ciberseguridad"**, dirigida a los funcionarios de la administración municipal, con el fin de fortalecer los conocimientos y medidas preventivas en el manejo seguro de la información institucional.

El evento se llevará a cabo en la siguiente fecha y horario:

- **Tema:** Buenas Prácticas en Ciberseguridad
- **Fecha:** Jueves **4 de diciembre**
- **Hora:** **10:30 a.m.**
- **Entidad orientadora:** Infortec – Especialistas en Ciberseguridad
- **Organiza:** Alcaldía de Pereira

Agradecemos contar con su participación puntual, dado que la ciberseguridad constituye un eje fundamental para la protección de los activos de información y la continuidad de los servicios institucionales.

Enlace de para la capacitación.

[https://teams.microsoft.com/join/19%3ameeting\\_Yzg2MjlxZjctM2Q3My00NWZjLTlkODctODIwNGQ4MGYyYTQ4%40thread.v2/0?context=%7b%22Tid%22%3a%22445f14c4-36aa-451d-8af5-79a215dfb961%22%2c%22Oid%22%3a%2256177758-e442-4c57-828a-68b0d1aac217%22%7d](https://teams.microsoft.com/join/19%3ameeting_Yzg2MjlxZjctM2Q3My00NWZjLTlkODctODIwNGQ4MGYyYTQ4%40thread.v2/0?context=%7b%22Tid%22%3a%22445f14c4-36aa-451d-8af5-79a215dfb961%22%2c%22Oid%22%3a%2256177758-e442-4c57-828a-68b0d1aac217%22%7d)

Id. de reunión: 221 725 709 336 79

Código de acceso: kq9be7Ls

Atentamente

**CARLOS FERNANDO GARCIA CAICEDO**  
**Director Operativo de Infraestructura Tecnológica**

Proyectó: GUSTAVO ADOLFO RIVERA GARCIA - Contratista - 0400 Secretaría de Tecnologías de la Información y la Comunicación

Anexos digitales: Buenas\_practicas.jpeg



# CHARLA DE BUENAS PRÁCTICAS DE CIBERSEGURIDAD

## Alcaldía de Pereira

ALEJANDRO PÉREZ GARCÍA

Consultor TI Infortec

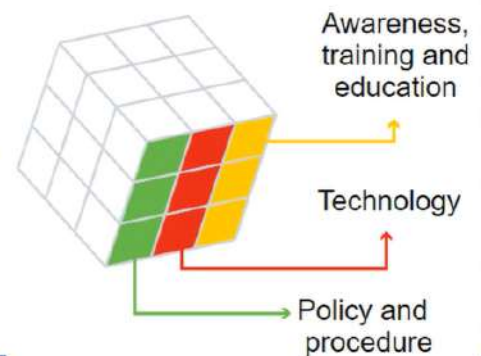
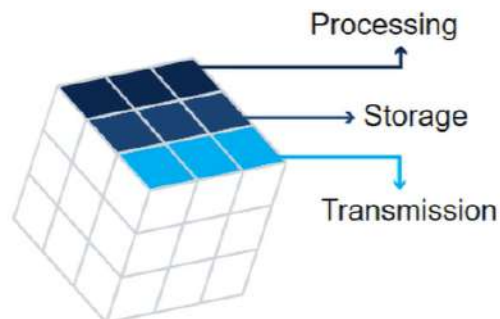
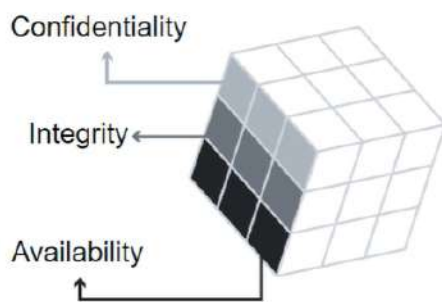
1. Usa la misma contraseña en más de 3 servicios.
2. Alguna vez han hecho clic en un enlace o abierto un archivo adjunto sin estar 100% seguros de quién lo envió.
3. Si usan o han usado redes WiFi públicas (cafés, aeropuertos).



4. Si alguna vez han ignorado una actualización de software.
5. Descargado apps fuera de las tiendas oficiales.
6. Guardan las contraseñas en el navegador.

# Base de la información digital

## Cubo de McCumber





## Qué es una amenaza cibernética?

- Las amenazas cibernéticas se refieren a cualquier actividad maliciosa llevada a cabo a través de medios electrónicos, con el objetivo de comprometer la seguridad de sistemas informáticos, redes, dispositivos o datos. Pueden ser llevadas a cabo por grupos, individuos o estados.

# Principales amenazas cibernéticas

Ingeniería social



Botnets



Descifrado de contraseñas



Ataques sobre el camino



Denegación de servicio (DoS)



Envenenamiento de optimización de motores de búsqueda



Ataques de contraseñas



# Síntomas Malware

- Un aumento en el uso de la unidad central de procesamiento (CPU), lo que ralentiza su dispositivo.
- Su computadora se congela o falla con frecuencia.
- Una disminución en la velocidad de navegación web.
- Problemas inexplicables con sus conexiones de red.
- Archivos modificados o eliminados la presencia de archivos, programas o iconos de escritorio desconocidos.
- Procesos desconocidos en ejecución.
- Programas que se apagan o reconfiguran solos.
- Correos electrónicos enviados sin su conocimiento o consentimiento.



## Qué es ingeniería social?

- Es un tipo de ataque que confía en la interacción humana, para engañar a la víctima y que esta brinde información sensible, o tome una acción que lo dañe a sí mismo o a su organización. Los ingenieros sociales comúnmente usan técnicas tales como phishing, pretexting, tailgating.





# Rol de inteligencia artificial



ChatGPT

Grok



Gemini

Apple Intelligence



**Campañas de Phishing:** Uso de IA para personalizar y ajustar dinámicamente ataques, aumentando la probabilidad de éxito al persuadir a las víctimas para que hagan clic en enlaces maliciosos, descarguen archivos o divulguen información confidencial.



**Compromiso del Correo Electrónico Empresarial:** IA imita el estilo de escritura de ejecutivos para enviar correos fraudulentos convincentes, engañando a empleados para que cumplan solicitudes ilegítimas.



**Phishing Selectivo (Spear Phishing):** Ataques focalizados que usan IA para recopilar datos específicos, imitar comportamientos y traducir mensajes, haciéndolos altamente personalizados y efectivos.



**Deepfakes Generados por IA:** Avances en IA producen deepfakes difíciles de detectar, capaces de causar pérdidas financieras y manipular la opinión pública, generando escepticismo sobre la autenticidad del contenido digital.

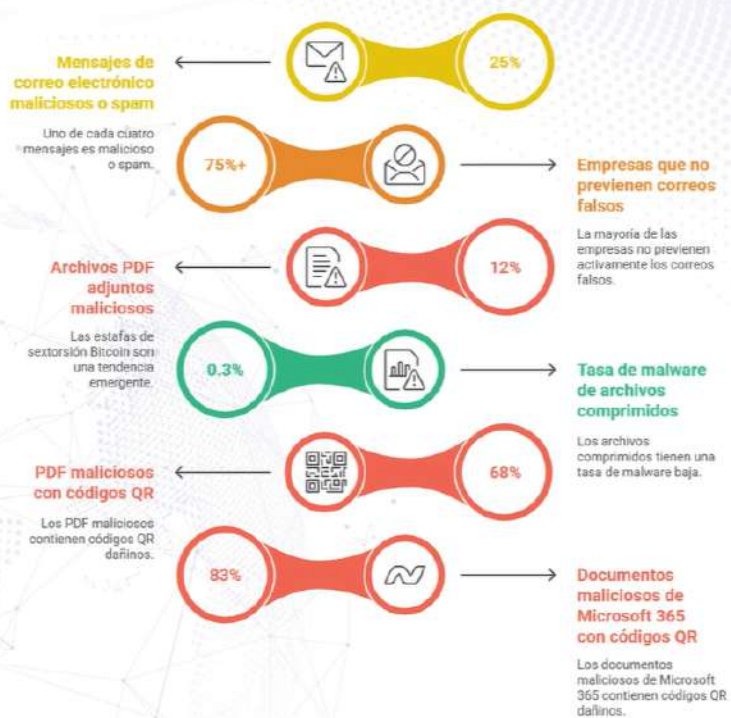


# Estafas Digitales comunes



- Soporte técnico
- Impostores
- Premios y loterías
- Trabajos o empleos
- Financieras

## Estadísticas de amenazas de correo electrónico



## Impacto de los Ataques de Correo Electrónico

Impacto en las organizaciones



# Es o no real? – Ejemplo 1

## Alerta informativa Sucursal Virtual

Mensaje enviado con importancia Alta.

SeguridadBancaVirtual@AppBancolombia.com <nelsonlubo@hotmail.com>  
Para: Usted

 Bancolombia

### Sucursal Virtual Personas

Bancolombia le informa 08/03/2023.

Hemos detectado un acceso no autorizado y movimientos inusuales en tu **Sucursal Virtual Personas** por motivos de seguridad bloqueamos preventivamente tus transacciones y clave dinámica. Actívala validando su identidad ingresando el código de seguridad de 6 dígitos que será enviado a tu número registrado o correo en nuestro sistema.

Ingresar en nuestra Sucursal virtual Personas para validar tu identidad para seguir utilizando nuestra APP

CONTINUAR

<https://bespoke-cat-a3f0d1.netlify.app>

 Bancolombia

# Es o no real? – Ejemplo 1

## Alerta informativa Sucursal Virtual

Mensaje enviado con importancia Alta.

SeguridadBancaVirtual@AppBancolombia.com <nelsonlubo@hotmail.com>  
Para: Usted

 Bancolombia

### Sucursal Virtual Personas

Bancolombia le informa 08/03/2023.

Hemos detectado un acceso no autorizado y movimientos inusuales en tu **Sucursal Virtual Personas** por motivos de seguridad bloqueamos preventivamente tus transacciones y clave dinámica. Actívala validando su identidad ingresando el código de seguridad de 6 dígitos que será enviado a tu número registrado o correo en nuestro sistema.

Ingresar en nuestra Sucursal virtual Personas para validar tu identidad para seguir utilizando nuestra APP

CONTINUAR

<https://bespoke-cat-a3f0d1.netlify.app>

 Bancolombia

# Es o no real? – Ejemplo 2

andresnavigator89 - Tienes (1) paquete esperando ser entregado 📦. Usa tu código para rastrearlo y recibirlo 📦. #ID63848 [D](#) [Spam x](#)

DHL 📦 <andresnavigator89@atwgwzcmjh.authmail.org>

para mí

¿Por qué e

No es s

de: **DHL 📦 <andresnavigator89@atwgwzcmjh.authmail.org>**  
para: andresnavigator89@gmail.com  
fecha: 7 oct 2025, 17:54  
asunto: andresnavigator89 - Tienes (1) paquete esperando ser entregado 📦. Usa tu código para rastrearlo y recibirlo 📦. #ID63848  
enviado por: **zandervolegost.authmail.org**  
firmado por: **atwgwzcmjh.authmail.org**  
seguridad: [Cifrado estándar \(TLS\)](#) [Más información](#)

**DHL**

**Tiene (1) paquete pendiente de entrega 📦. Use su código para rastrearlo y recibirlo.**

**Su código de rastreo es:**

083164538

[Continuar >](#)

Programa su entrega y suscríbese a las notificaciones de calendario para evitar incidentes similares en el futuro.

[Programar Entrega 📦](#)

Gracias por su pronta atención a este asunto. Esperamos su confirmación.

Atentamente,  
DHL

[Soliré resolver](#) | [Contacto](#) | [Gestionar preferencias](#)

© 2025 DHL S.A. Todos los derechos reservados.



## infopratique.my.be no admite una conexión segura con HTTPS

Esta advertencia aparece porque este sitio no admite HTTPS y está usando el modo privado. [Más información acerca de esta advertencia](#)

[Ir al sitio](#)

[Volver](#)

Remitente  
sospechoso

Asunto  
alarmante



### Correo electrónico sospechoso



soporte@micr0soft.com

Tu cuenta será bloqueada en 24 horas

Enlace  
sospechoso



Estimado(a) usuario,

Su cuenta será tu loqueadelo con  
este nonector pice.

Por fobaer inmunedo.

Atentamente,

El equipo de soporte



**Subject:** DHL -AWB Shipment Has Arrived  
**To:** Recipients <dhl@lupends.com>  
**From:** DHL Customer Support (dhl@lupends.com) <dhl@lupends.com>  
**Date:** 06/04/2019 07:50 PM

iii¡RECORDATORIO!!!

Querido Cliente,

Intentamos entregar tu ítem a las 2:30 pm el 24 de Mayo de 2019 (leer los detalles en el archivo adjunto).  
 La entrega falló porque nadie estaba presente en la dirección de entrega, por lo que esta notificación fue automáticamente enviada.

Si la entrega no es reprogramada o el paquete retirado dentro de las 72 horas, será devuelto a su emisor.

Número de envío: (leer los detalles en el archivo adjunto).  
 Clase: envío de paquetes  
 Servicio: (leer los detalles en el archivo adjunto).  
 Estado: envío de notificación por correo electrónico.

Leer los detalles en el archivo adjunto.

**Destinatario genérico**  
**Dominio DHL falso (Mdaemon muestra el verdadero entre llaves para ayudar al usuario a identificar falsificación de identidad)**  
**Falsa urgencia**  
**Saludo genérico**  
**Intento de convencer al receptor de abrir el archivo adjunto**  
**Intento de convencer al receptor de abrir el archivo adjunto**  
**Intento de convencer al receptor de**





## Buenas prácticas

- No hacer clic en enlaces o archivos adjuntos de origen desconocidos.
- Evitar usar redes wifi-públicas o abiertas sin el uso de una VPN
- Usar contraseñas más seguras y difíciles de descifrar.
- Mantener actualizados los dispositivos (*software* y sistema operativo).
- Usar herramientas de seguridad como antivirus y llaveros
- Establecer la autenticación de dos factores.
- No instales aplicaciones móviles de fuentes inseguras.
- No descargues software enviado por desconocidos.
- No descargues aplicaciones de fuentes desconocidas.
- No conectes USBs conectadas por "casualidad" en tu ordenador
- Siempre verifica.

# Contraseñas seguras

- Longitud mayor a 12 caracteres
- Incluye mayúsculas, minúsculas, números y caracteres especiales.
- Evita incluir información personal en la contraseña
- No reutilices la misma contraseña en diferentes sitios
- Crea contraseñas a partir de frases, que sean fáciles de recordar. (libros, canciones, lugares)
- Evita patrones fácilmente adivinables (qwerty, 123456, 1q2w3e4r5t)
- Evita secuencias lógicas.

## Ejemplo práctico de creación de una contraseña segura:

Paso 1: Selecciona una frase memorable.

Ejemplo: "**Me encanta ver series de netflix**".

Paso 2: Transforma la frase utilizando sustituciones:

Reemplaza letras por números y símbolos similares:

o "a" por "@"

o "e" por "3"

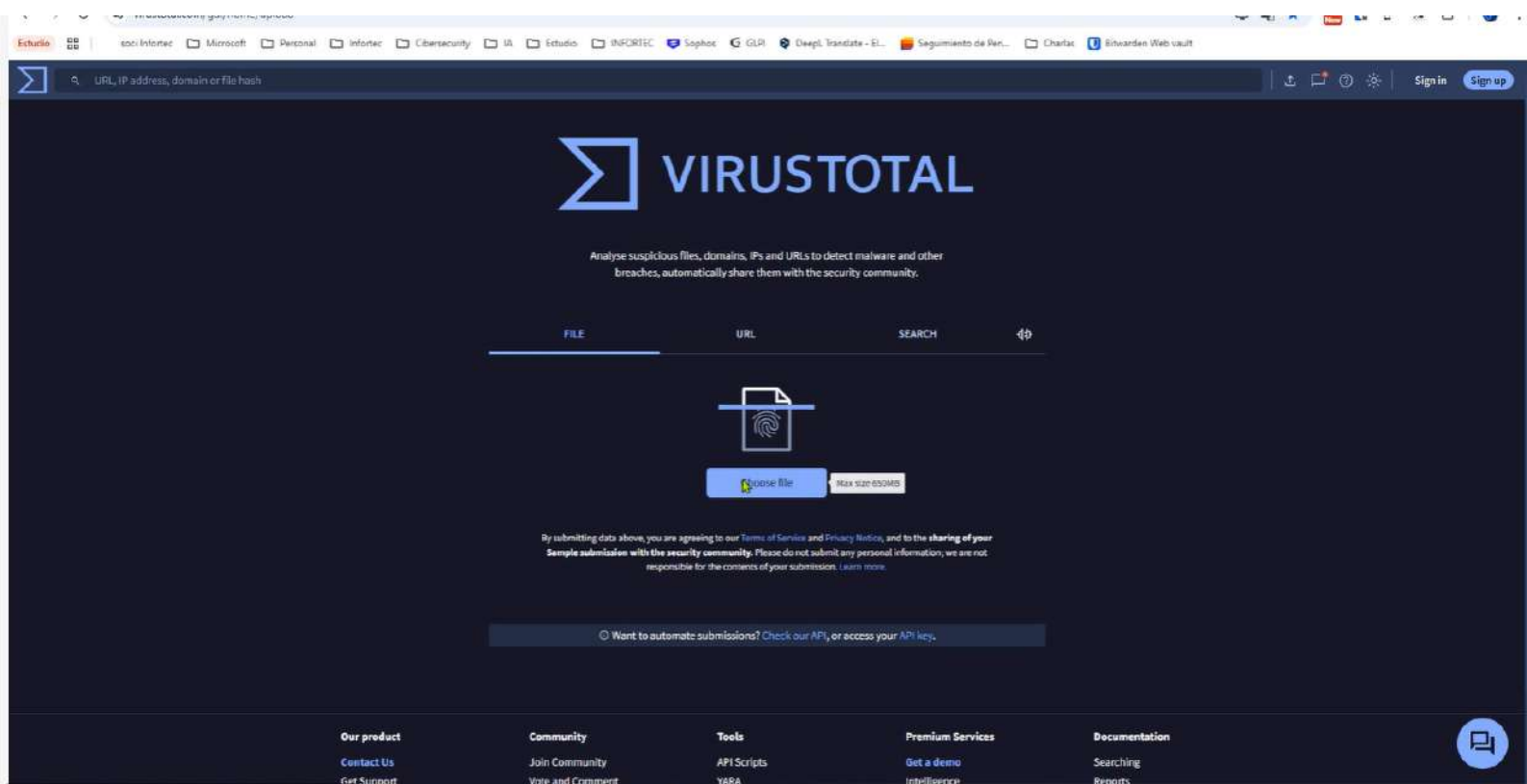
o "i" por "1"

o "o" por "0"

o "s" por "\$"

Paso 3: Aplica mayúsculas y minúsculas y agrega símbolos:

**M3Enc@nt@v3rs3r13sd3n3tfl1x**



7b56d9a4ac698e1d6cc4ab7d9b5b5f9244e20a0692d82d48500051ff0f529a51

#### Certificate Subject

|                     |                                                   |
|---------------------|---------------------------------------------------|
| Distinguished Name  | C:34, CN:magisapp, L:RT, O:magis, ST:SP, OU:magis |
| Common Name         | magisapp                                          |
| Organization        | magis                                             |
| Organizational Unit | magis                                             |
| Country Code        | 34                                                |
| State               | SP                                                |
| Locality            | RT                                                |

#### Certificate Issuer

|                     |                                                   |
|---------------------|---------------------------------------------------|
| Distinguished Name  | C:34, CN:magisapp, L:RT, O:magis, ST:SP, OU:magis |
| Common Name         | magisapp                                          |
| Organization        | magis                                             |
| Organizational Unit | magis                                             |
| Country Code        | 34                                                |
| State               | SP                                                |
| Locality            | RT                                                |

#### Permissions

- △ android.permission.WRITE\_EXTERNAL\_STORAGE
- △ android.permission.POST\_NOTIFICATIONS
- △ android.permission.READ\_EXTERNAL\_STORAGE
- △ android.permission.READ\_MEDIA\_IMAGES
- △ android.permission.READ\_MEDIA\_AUDIO
- △ android.permission.CAMERA
- △ android.permission.REQUEST\_INSTALL\_PACKAGES
- △ android.permission.MANAGE\_EXTERNAL\_STORAGE
- ① android.permission.CHANGE\_NETWORK\_STATE
- ① com.huawei.android.launcher.permission.CHANGE\_BADGE
- ① android.permission.BLUETOOTH
- ① android.permission.ACCESS\_WIFI\_STATE
- ① android.permission.INTERNET
- ① android.permission.GET\_TASKS
- ① com.google.android.c2dm.permission.RECEIVE
- ① android.permission.ACCESS\_NETWORK\_STATE
- ① android.permission.CHANGE\_WIFI\_MULTICAST\_STATE

## Recursos útiles

- **Escaneo de páginas y archivos:**
  - <https://www.virustotal.com/gui/home/url>
  - <https://urlscan.io>
  - <https://safeweb.norton.com>
- **Chequea tu correo:**
  - <https://haveibeenpwned.com>
- **Chequea tu contraseña:**
  - <https://bitwarden.com/password-strength/>
- **Entrenamientos**
  - <https://phishingquiz.withgoogle.com>

