



Escuela Tecnológica Instituto Técnico Central

Establecimiento Público de Educación Superior

Capacitación en **Microsoft 365** *y Uso Responsable del Correo Electrónico*

OBJETIVOS

De la capacitación

- Aplicar buenas prácticas de seguridad en el uso del correo institucional.
- Identificar amenazas de ciberseguridad comunes.
- Proteger la información institucional.
- Utilizar de manera segura las herramientas colaborativas de Microsoft 365.
- Reconocer y reportar incidentes de seguridad de la información.

Grabación



**Escuela Tecnológica
Instituto Técnico Central**
Establecimiento Público de Educación Superior

Correo electrónico

¿Por qué es Importante?

El correo electrónico continúa siendo uno de los principales medios utilizados para la distribución de amenazas informáticas.

Los atacantes buscan:

- Robar credenciales.
- Obtener información sensible.
- Distribuir malware.
- Realizar fraudes mediante suplantación de identidad.

Pregunta:

¿Cuántos correos electrónicos recibe diariamente?

- Menos de 20
- Entre 20 y 50
- Más de 50





Estadísticas de Ciberseguridad

Tendencias Globales



Más del
90%
de los incidentes
comienzan mediante
correo electrónico.



El **phishing**
sigue siendo uno de
los métodos más
utilizados por los
atacantes.



El robo de
credenciales
es una de las principales
causas de incidentes
de seguridad.



El **error humano**
continúa siendo uno de
los factores más relevantes
en los incidentes de
seguridad de la información.



Reflexión

La mejor herramienta de seguridad sigue siendo
un usuario informado y consciente.



Escuela Tecnológica
Instituto Técnico Central
Establecimiento Público de Educación Superior

La Información Como Activo Institucional

La información es uno de los activos más importantes de la ETITC.

Tipos de información institucional

- Académica
- Administrativa
- Financiera
- Talento humano
- Investigación
- Proyección social
- Información de estudiantes

Reflexión

La seguridad de la información no depende únicamente de la tecnología; depende también del comportamiento de las personas.



Ecosistema Microsoft 365

Microsoft 365 proporciona un entorno integrado de productividad y colaboración.

Herramientas Principales

Outlook

Gestión de correo electrónico y calendario.

OneDrive

Almacenamiento seguro de archivos.

Teams

Comunicación y colaboración.

SharePoint

Gestión documental institucional.

Word Online

Documentos colaborativos.

Excel Online

Análisis de información.

Forms

Creación de formularios y encuestas.



Uso Seguro de OneDrive

Ventajas

- Respaldo automático.
- Disponibilidad desde cualquier lugar.
- Sincronización segura.

Evitar

- Uso de USB no autorizados.
- Almacenamiento en el medios personales.
- Copias de trabajo fuera de entornos institucionales.

Microsoft Teams

Ventajas

- ✓ Comparte de forma segura
- ✓ Colabora en tiempo real
- ✓ Protege la información institucional

Riesgos

- ✗ Fuga de información
- ✗ Falta de trazabilidad
- ✗ Dificultades en auditorías
- ✗ Pérdida del conocimiento institucional
- ✗ Menor productividad y colaboración
- ✗ Incumplimiento de políticas institucionales



Escuela Tecnológica
Instituto Técnico Central
Establecimiento Público de Educación Superior

Contraseñas Seguras

Capacitación en
Microsoft 365
y Uso Responsable del
Correo Electrónico



Características

- ✓ Largas.
- ✓ Únicas.
- ✓ Difíciles de adivinar.
- ✓ Fáciles de recordar.



Ejemplo

Escue1a e+ic*



Evitar

123456
password
admin123
ETITC2026



Autenticación Multifactor (MFA)

¿Qué es?

Mecanismo de seguridad que utiliza dos o más factores para validar la identidad.

Ejemplos

- Contraseña.
- Aplicación Authenticator.
- Código SMS.
- Token.

Beneficio

Aunque un atacante conozca la contraseña, no podrá acceder fácilmente a la cuenta.

Capacitación en
Microsoft 365
y Uso Responsable del
Correo Electrónico



**Escuela Tecnológica
Instituto Técnico Central**
Establecimiento Público de Educación Superior

Uso Correcto del Correo Institucional

Permitido

- Comunicaciones institucionales.
- Procesos académicos.
- Actividades administrativas.
- Comunicación oficial.

No Permitido

- Autenticación en aplicaciones y servicios.
- Spam.
- Información personal no autorizada.



Recomendaciones Correo Electrónico

Buenas Prácticas

★ Hacer

- ✓ Verificar remitentes
- ✓ Revisar dominios
- ✓ Desconfiar de mensajes urgentes
- ✓ Validar adjuntos
- ✓ Reportar correos sospechosos

★ Evitar

- X Compartir contraseñas
- X Abrir archivos desconocidos
- X Hacer clic en enlaces sin validar
- X Utilizar correos personales para información institucional



Anatomía de un Correo Phishing

Señales de Alerta

- Dirección de correo sospechosa.
*Servicioalcliente**banco**lombia@gmail.com*
- Errores ortográficos.
*www.Banc**0**lombia.com*
- Mensajes alarmantes o urgentes.
“Su capacidad de almacenamiento....”
- Solicitudes de contraseñas.
“Hubo una actualización del sistema....”
- Archivos adjuntos inesperados.
.exe, .msi, .bat, .vbs



Verificación de Enlaces

Antes de hacer clic:

Revisar URL

Ejemplo seguro:

<https://login.microsoftonline.com>

Ejemplo sospechoso:

<https://micr0soft-online.com>

Recomendación

Siempre posicionar el cursor sobre el
enlace antes de abrirlo.



Ingeniería Social

Principales Técnicas

Phishing

Correos fraudulentos.

Vishing

Llamadas telefónicas fraudulentas.

Smishing

Mensajes de texto fraudulentos.

Spear Phishing

Ataques dirigidos a una persona específica.

Ejercicio Práctico

Situación

Recibe una llamada indicando que pertenece al área de tecnología y le solicitan:

- Usuario institucional.
- Contraseña.
- Código MFA.

¿Qué haría?



Ejercicio Práctico No. 1

Caso

Recibe el siguiente correo:
Su cuenta institucional será suspendida en
30 minutos.
Ingresa inmediatamente para validar su
contraseña.

Preguntas

¿Qué señales de alerta identifica?
¿Qué acción tomaría?

Capacitación en
Microsoft 365
y Uso Responsable del
Correo Electrónico



**Escuela Tecnológica
Instituto Técnico Central**
Establecimiento Público de Educación Superior

Caso de Estudio

Escenario

Recibe un correo con asunto:
Factura pendiente de pago
Adjunto:
Factura.zip

Analice

- Riesgos identificados.
- Acciones recomendadas.
- Procedimiento de reporte.

Capacitación en
Microsoft 365
y Uso Responsable del
Correo Electrónico



**Escuela Tecnológica
Instituto Técnico Central**
Establecimiento Público de Educación Superior

¿Qué Hacer Ante un Incidente?

★ Pasos

1. No responder.
2. No eliminar evidencias.
3. Tomar captura de pantalla.
4. Reportar inmediatamente.
5. Informar a la Mesa de Servicios o Seguridad de la Información.



Top 10 Recomendaciones

1. Utilice MFA.
2. Mantenga actualizado su equipo.
3. Verifique remitentes.
4. Proteja sus contraseñas.
5. Use OneDrive institucional.
6. Evite USB no autorizados.
7. Reporte correos sospechosos.
8. Revise los enlaces antes de hacer clic.
9. Clasifique correctamente la información.
10. Consulte cuando tenga dudas.



Compromiso de Seguridad



La seguridad de la información es responsabilidad de todos.

Cada funcionario, docente, contratista y estudiante contribuye a la protección de la información institucional mediante el uso adecuado de las herramientas tecnológicas.



GRACIAS

Capacitación en
Microsoft 365 
*y Uso Responsable del
Correo Electrónico*

Sitio Web:

WWW.ETITC.EDU.CO

Redes sociales:

@ETITC



**Escuela Tecnológica
Instituto Técnico Central**
Establecimiento Público de Educación Superior