



**ZURICH**<sup>®</sup>

**En Zurich protegemos el esfuerzo  
de los ecuatorianos para asegurar  
el futuro del país...**

**Hagámoslo Juntos**

# Zurich Insurance Group

## Construyamos el futuro juntos



Estamos aquí para juntos alcanzar las metas propuestas.



# Cyberseguridad en tiempos de teletrabajo



**Introducción**

**¿Cuál es la situación actual del riesgo cibernético?**

**¿Cómo ocurren los ataques?**

**Consejos de seguridad cibernética**

# Cyber Risk Engineering Network



# Ciberamenazas: Objetivos de Ciberataques








	Cadena de suministro		Registros de empleados
	Fuente de alimentación		Contraseñas de cuenta de servicio débiles
	Máquina de procesos automatizados		Contraseñas de cuenta privilegiadas débiles
	Propiedad intelectual		Datos sin cifrar
	Información financiera		Red única no segmentada
	Información al cliente		Comunicaciones externas
	Demografía propietaria		Extorsión de rescate

# Ciberamenazas: Fuentes de Amenazas

	Error humano		Correos de suplantación
	Empleados remotos		Descargas
	Ex empleados maliciosos		Dispositivos USB infectados
	Dispositivos móviles perdidos		Escaneo remoto de red
	Vendedores / Proveedores		Contraseñas repetidas débiles
	Ataques de estado		Conectarse a wifi abierto

# Ciberamenazas: Consecuencias

	Interrupción del negocio
	Pérdida de ingresos
	Pérdida de clientes
	Daño a la propiedad
	Servicios de productos defectuosos
	Transacciones inexactas

	Pérdida de información irrecuperable
	Vulnerabilidad de reputación
	Preocupaciones de los inversores / precio de las acciones
	Preocupaciones de los empleados
	Costo de reemplazo de datos
	Responsabilidades legales regulatorias
	Costos de forense



# Datos relevantes: Estadísticas a considerar



**243**

Número medio de días que los ataques avanzados están en la red antes de ser detectados

**70%**

Porcentaje de incumplimientos asociados con actores de estados nacionales o afiliados al estado involucrados en phishing

**2.9 billones**

Registros filtrados en 2017 (esto solo cuenta las infracciones divulgadas públicamente)

**23%**

Porcentaje de usuarios que comparten sus contraseñas de red con colegas

**28%**

Probabilidad de una transgresión material recurrente en los próximos dos años

**10%**

Porcentaje de credenciales de correo electrónico de empleados de Fortune 500 en la web oscura

**Contraseñas Comunes**

"123456," "password," "!@#\$%^&," "qwerty," "12345,"  
"123456789," "aa123456," "1234567," "fútbol,"  
"iloveyou," "admin," "Tequiero," "mariposa," "login,"  
"abc123," "estrella," "654321," "bonita," "Contraseña"

**\$148**

Costo promedio por registro perdido o robado

**58%**

Porcentaje de víctimas clasificadas como pequeñas empresas



ZURICH<sup>®</sup>

# Cyber riesgos en el mundo del teletrabajo

# La dimensión cibernética del coronavirus

Empresas enfocadas en mantener el control

Más trabajo desde casa o usando redes remotas

Nueva ola de ataques cibernéticos

Mayor probabilidad de hacer click en archivos maliciosos o utilizar redes no seguras

Ciber criminales se benefician del desconocimiento

Hay miedo y mayor distracción



- Aumento en el último mes en ciberataques: tanto en frecuencia como en cantidad (iconos en cada bullet que represente lo que es cada uno)
- Pérdida de conciencia en la seguridad por distracciones no convencionales
- Ataques con archivos maliciosos sobre el COVID-19. Aprovechan pánico y desinformación de la gente
- Los trabajadores de las empresas no entienden la magnitud de los riesgos



# Highlights del ciberriesgo



**500%**

Más ataques cibernéticos desde COVID-19 empezó

**93%**

Aumento de las violaciones de datos por errores humanos

**5%**

Inversión en Ciberseguridad (IBM)

**US\$ 86K  
1.7M**

Valor promedio de un ataque (P~G empresas)

**US\$ 600  
Billones**

Cifra total em 2019 (WEF)

**US\$ 3  
Trillones**

Cifra total hasta 2021 (WEF)



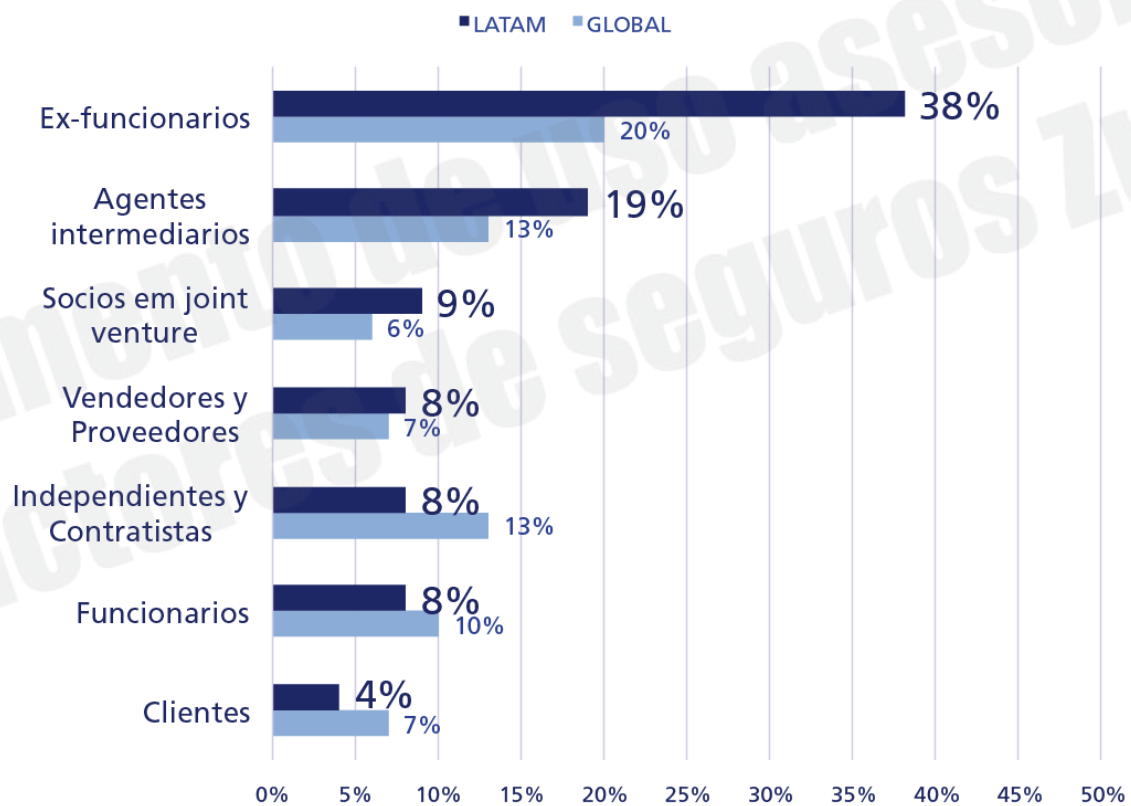
ZURICH<sup>®</sup>

¿Como ocurren  
los ataques cibernéticos?

# Desmitificación de las amenazas digitales



## Principales medios de acceso



# Tipos de ataques Ciberneticos



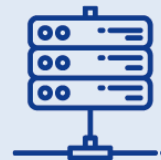
Phishing



Business Email  
Compromise (BEC)



Ingeniería  
social



Ramsoware

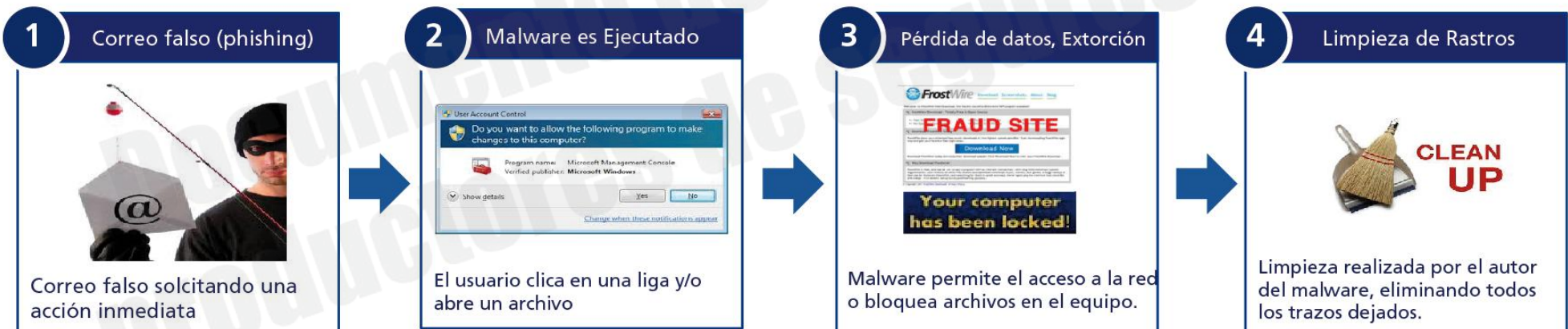


Documento de consulto asesores Zurich  
productores de seguros Zurich



# Phishing

Comunicación fraudulenta a través de correos electrónicos con información específica sobre el destinatario para engañarlo mediante un click en un link o ejecución de un archivo para obtener los datos o accesos.



# Business Email Compromise (BEC)

Correos electrónicos suplantando personas de altos mandos de la organización para realizar transferencias electrónicas, no convencionales.

También conocido como Fraude del CEO o Man-in-the-Email attack.



# Ingeniería Social

Manipulación psicológica para obtener información confidencial mediante diferentes sistemas o aplicaciones.



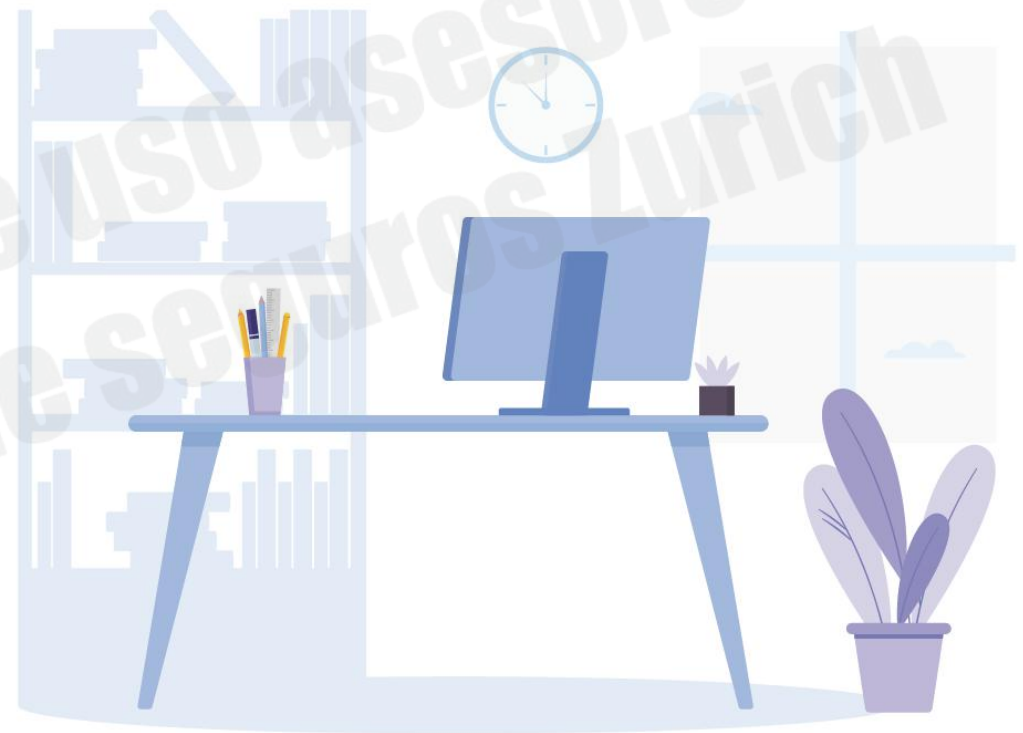


ZURICH®



Medidas Preventivas  
Formas de mitigar los ataques

Home Office no quiere decir que tu computador portátil corporativo pueda ser usado como tu computadora personal o el de tu familia.



## Lo que deberían hacer:

- Capacitaciones de seguridad informática.
- Informe cualquier contenido sospechoso a la mesa de ayuda de la compañía
- Informe pérdida de equipos al área responsable

## Lo que debes saber:

- Evitar y denunciar el Phishing
- Identificar contenido sospechoso
- No haga clic en enlaces sospechosos
- No abra archivos no solicitados
- No envíe información personal o financiera

## Seguridad de red local (residencial)

- Cambie la contraseña del enrutador y módems
- Use el cifrado WPA2
- Actualice el firmware de su enrutador
- Deshabilite la función "Administración remota"
- Ocultar el nombre de su red Wifi ("Ocultar nombre SSID")

## Seguridad de los dispositivos

- No use los dispositivos de la compañía para actividades recreativas
- Proteja dispositivos y documentos como si estuvieran en su oficina
- No imprima documentos de la empresa en casa

## Conexión y autenticación segura

- A través de conexiones VPN (red privada virtual) / Citrix / Etc.
- Empleo de una herramienta de autenticación en dos pasos / etapas (2FA / MFA)

## Concienciación de empleados/usuarios

- Política de seguridad de la información, clasificación de datos
- Entrenamiento y pruebas de Phishing e Ingeniería Social
- Entrenamiento específico para la seguridad durante el trabajo remoto

## Seguridad de la red

- "Firewall" actualizado ("Patched") y reglas revisadas
- Tener la herramienta NAC (Control de acceso a la red)
- Escaneos de Vulnerabilidad y "Pentests"

## Seguridad de los dispositivos

- "White/Black Listing" (aplicaciones y contenido)
- Bloqueo de puertos USB / comunicaciones externas
- Antivirus actualizado ("Patched")
- Sistemas operativos actualizados ("Patched")
- Gestión remota de equipos por MDM (Gestión de dispositivos móviles)
- Cifrado de disco (FDE)

## Mayor y mejor supervisión

- Monitoreo de red 24/7/365 (SOC / MSSP)
- Colección, Correlación and Análisis de registros (SIEM)
- Implemente bloqueos a sistemas que no sean necesarios y/o que no se pueda acceder de forma remota
- Bloquee temporalmente accesos remotos, no necesarios

## Migración en la nube

- "Cloud" no es sinónimo de seguridad
- La configuración de seguridad es esencial.
- Monitoreo de desviaciones y cambios no autorizados a la configuración

## ¿Qué pasa con las herramientas oficiales de comunicación?

- Email (filtros de "Malware"/"Spam"/"Phishing")
- Smartphones (MDM)
- Herramientas de mensajería Skype / Whatsapp /etc.
- Herramientas de mensajería (Skype / Teams / Webex / Zoom / etc.).
- Contenido anexo

## Controles sobre los canales de comunicación oficiales.

- Help Desk (Soporte a colaboradores).
- Call Center (Soporte a clientes).
- Canales electrónicos (websites, redes sociales, etc)



## PARE, PIENSE, PROCEDA:



Cuando dude, juegue fuera



Piense antes de actuar



Proteja su contraseña



Cuenta única, contraseña única

Documento de uso asesores  
Productores de seguros Zurich

Ciber



Seguridad Riesgo  
Protección Prevención

El futuro  
dependerá de  
lo que hagamos  
Hoy



ZURICH<sup>®</sup>

¿Dudas & Preguntas?



**ZURICH**

®

Documento de Asesores  
productores seguros Zurich

