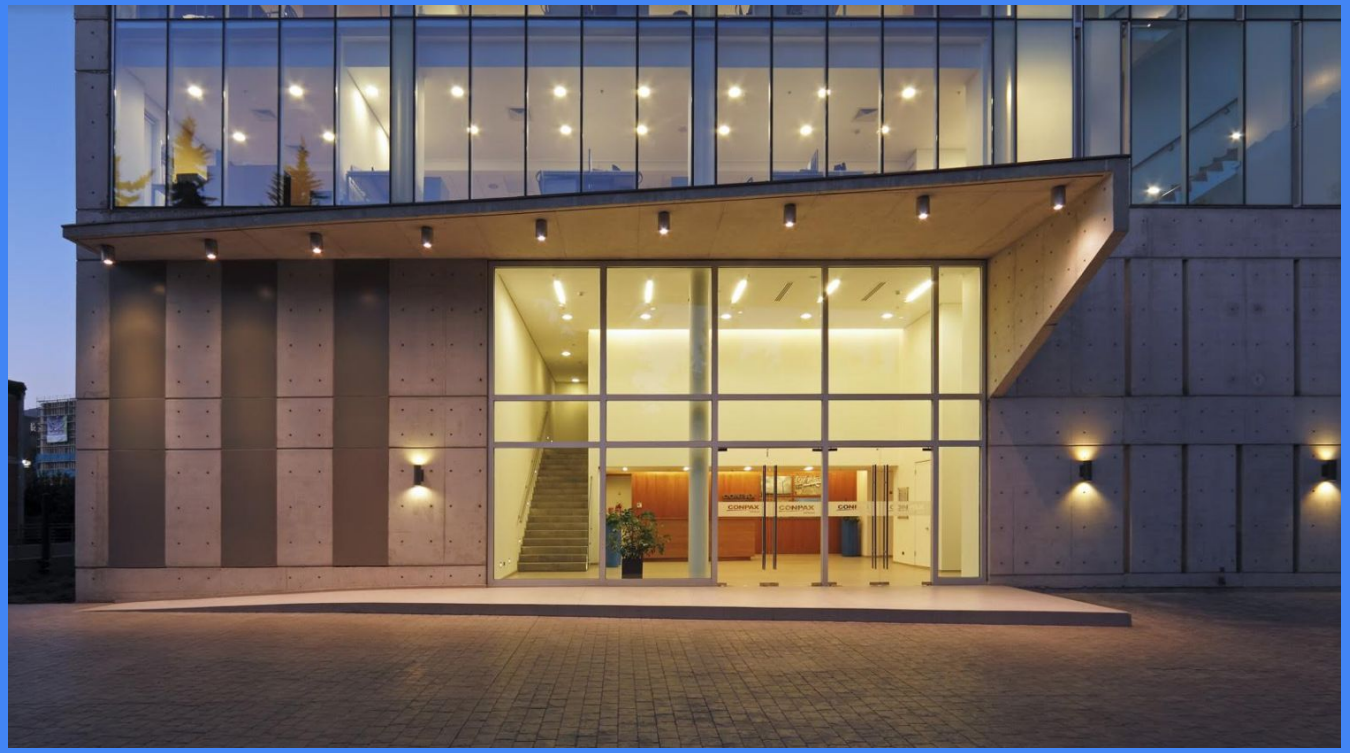


Charla Seguridad Informática

Equipo
Conpax TIC
26/03/2020

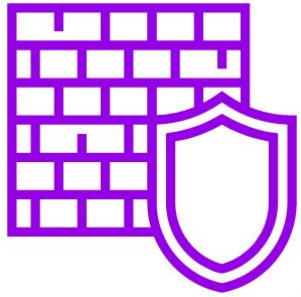
Dinko Yaksic

¿Qué es **Seguridad Informática?**

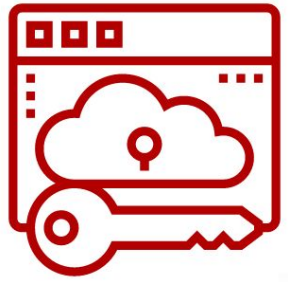
Protección de activos de información

- Confidencialidad
  - Privacidad
  - Identificación v/s Autenticación
- Integridad
  - Coherencia
  - Presencia
- Disponibilidad
  - Acceso
  - Acceso controlado

Física



Lógica

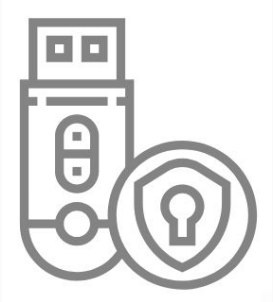


Pilares de la **Seguridad en el Acceso de Datos**

Un buen sistema de identificación + autenticación al que se tiene que tender, antes de otorgar privilegios, debería exigir al usuario:

- Algo que sepa

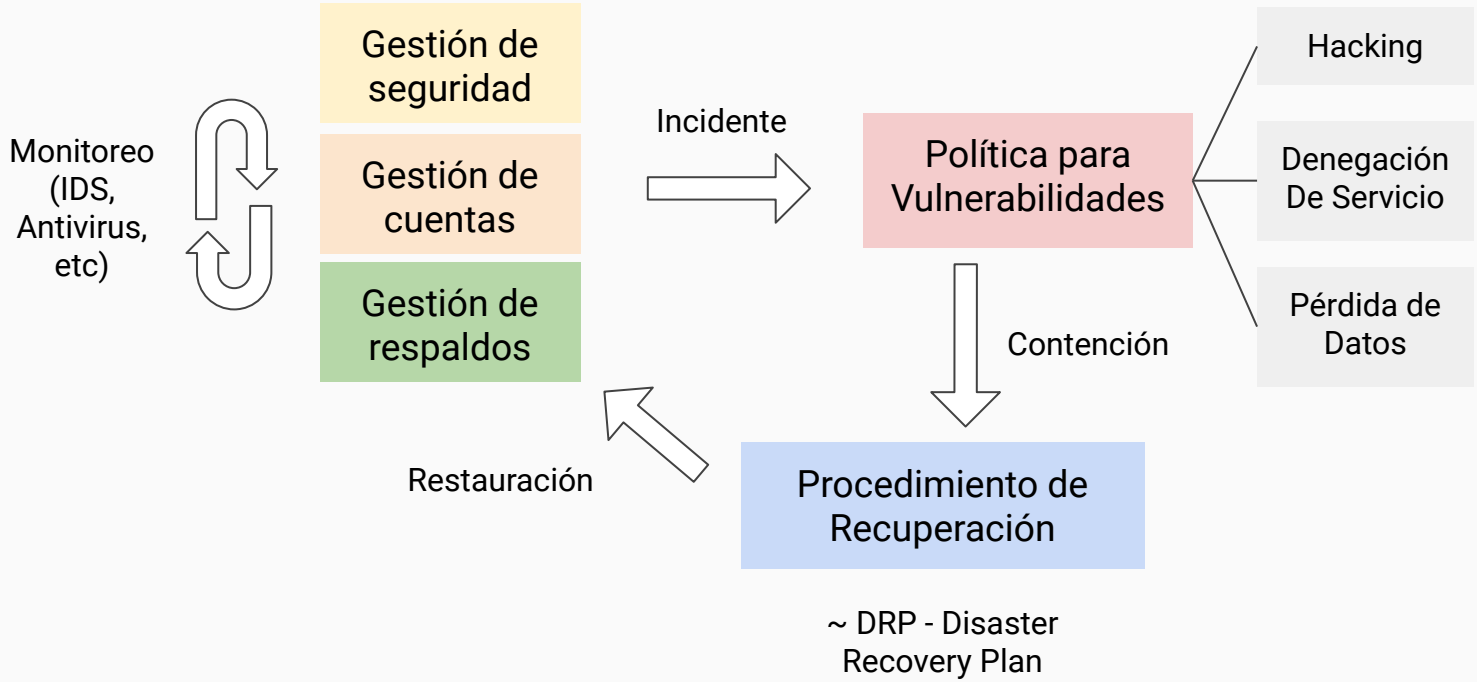
- Algo que tenga



- Algo que sea

Ciclo Operativo de **Seguridad Informática Organizacional**

- Secuencia de actividades relativas a seguridad de datos permanentes en la organización



Datos interesantes sobre **Seguridad Informática** (y I)

Crackers atacan un sitio cada 39 segundos

Universidad de Maryland

Se estima gasto mundial de US$ 134 Bn para 2022

Gartner

60% de los sitios maliciosos están vinculados a spam

Cisco

⅓ de los ataques involucran actores internos

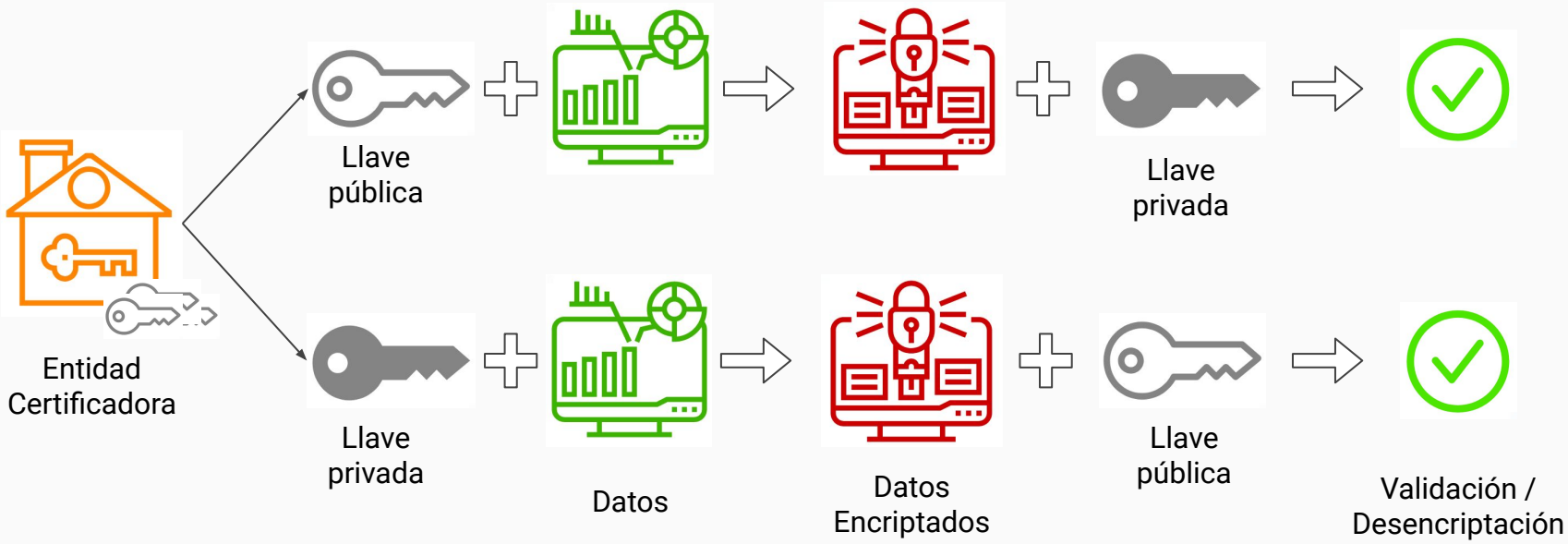
Verizon

Gobierno, retail y tecnología conforman el 95% de los rubros crackeados

Tech Republic

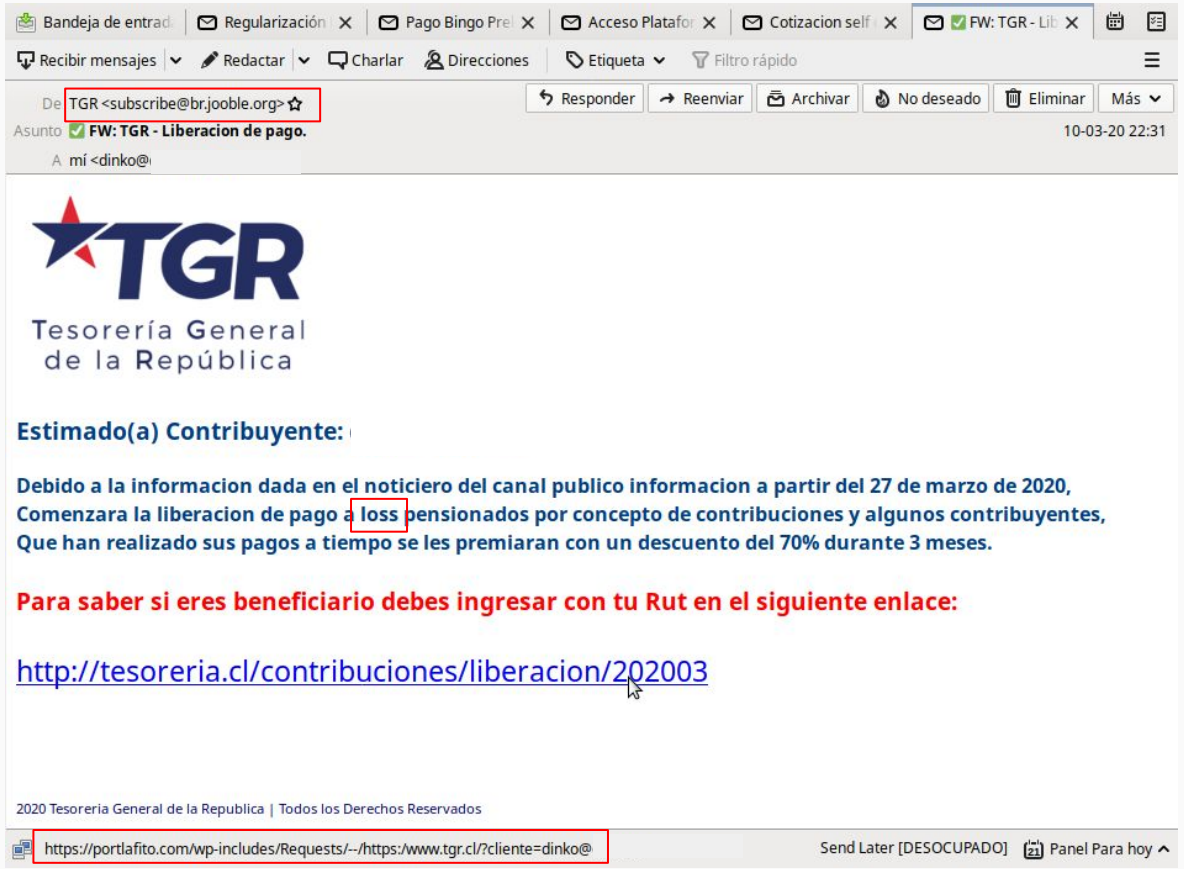
Concepto: **Firma Digital**

- Sistema criptográfico que permite identificar unívocamente e irrefutablemente la aceptación de un individuo c/r a un documento (o datos, en general)



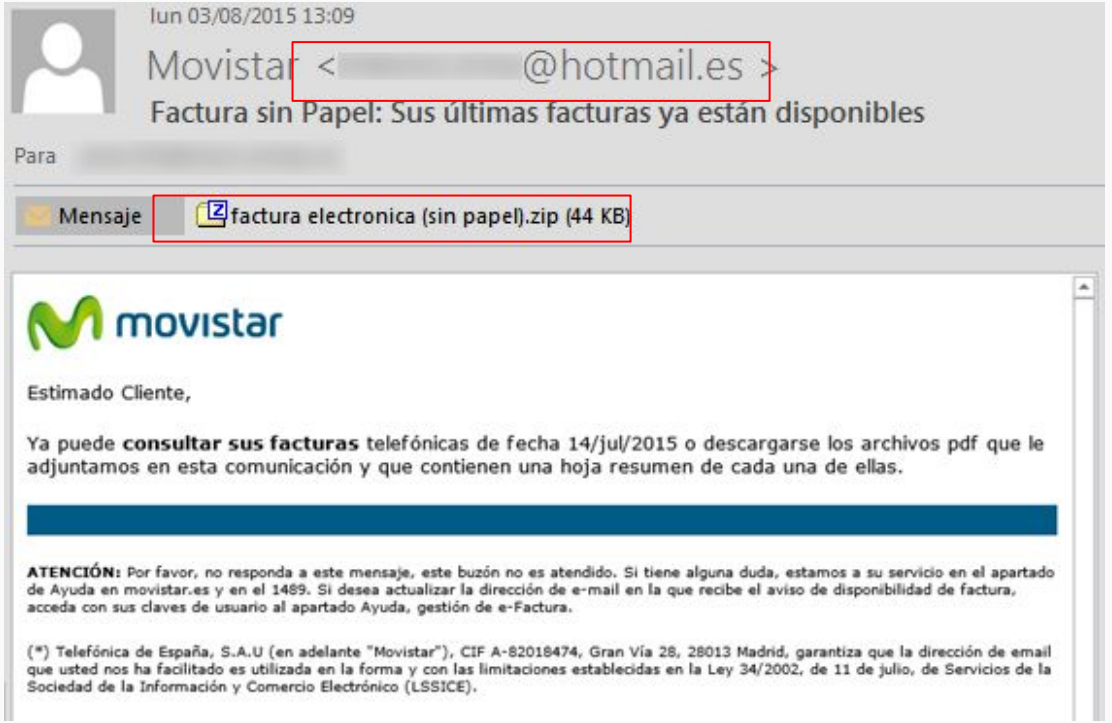
Concepto: **Phishing**

- Suplantación de un correo o sitio web
- Generalmente vinculados a *spam* (UCE - Unsolicited Commercial Email)
- Contramedidas:
  - Fijarse en la dirección web o remitente de correo. No confiar aunque sean conocidos
  - Buscar mal diseño, errores ortográficos, etc.



Concepto: **Malware**

- Lo que antes se conocía como “virus” o “troyano”: programa diseñado para ser nocivo
- Generalmente adjuntos a correo sospechoso
- Extensiones típicas:
  - Ejecutables: EXE, PIF, VBS, JS
  - Comprimidos (ZIP, RAR)
  - Planillas (XLS, XLSX)
  - Documentos (DOC, DOCX, PDF)



Concepto: **Ransomware**

- Tipo de malware, particular% dañino:
  - Recorre cada archivo de dato en el equipo (planilla, documento, imagen) y los encripta con un algoritmo muy complejo
  - Deja mensaje indicando cuenta **bitcoin** para obtener la llave de desencriptación
- Detección:
  - Equipo muy lento, con pocas aplicaciones abiertas
  - Uso intensivo del disco duro
  - Archivo antes accesible, ahora aparece solo “ruido”
- Medidas:
  - Apagar inmediatamente el equipo y no encender
  - Entregar equipo a expertos

Datos interesantes sobre **Seguridad Informática** (y II)

Compañías que han sido crackeadas: Facebook, Microsoft, Amazon, Adobe

IdentityForce

El costo promedio de una vulnera-bilidad importante es US$ 4 Mn

IBM

Motivación: financiera 70%, espionaje 25%

Verizon

6 meses promedio toma detectar una vulnerabilidad

ZDNet

95% brechas provienen de errores humanos

Information Management

Buenas Prácticas: Contraseñas realmente seguras

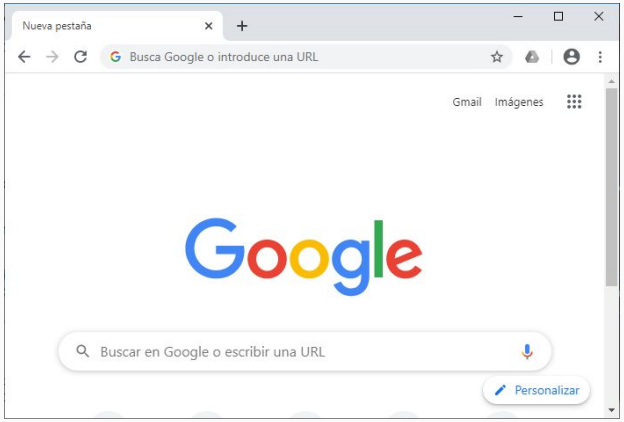
- La seguridad de una contraseña es proporcional a su complejidad
- Asumiendo un computador que puede probar 1 millón de contraseñas por segundo por “fuerza bruta”:
  - 8 dígitos:
    - 10^8 = 100 millones de combinaø → 100 segundos en crackear
  - 8 letras minúsculas o dígitos:
    - $(26 + 10)^8$ ~ 3 billones combinaø → 32 días
  - 8 letras minúsculas, mayúsculas o dígitos
    - $(26 + 26 + 10)^8$ ~ 218 billones combinaø → 7 años
  - 8 letras minúsculas, mayúsculas, dígitos o símbolos
    - $(26 + 26 + 10 + 20)^8$ ~ 2044 billones combinaø → 65 años

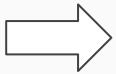
Buenas Prácticas: Dispositivos móviles

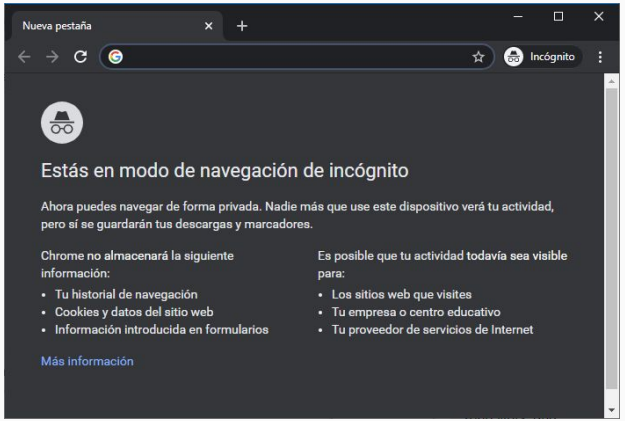
- No descargar Apps desde Google Play o Apple Store que no sean de fuentes confiables, ni estrictamente necesarias
- No seguir enlaces, ni descargar archivos desconocidos (que mayormente provienen desde chats)
- Establecer una contraseña de bloqueo de pantalla (o también patrón, o PIN)
- Deshabilitar ubicación: Es discutible. Tiene sus ventajas (*tracking*) y desventajas (*advertising*)

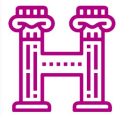
Buenas Prácticas: Navegación privada

- Browsers en orden de seguridad: Chrome, Firefox, Edge, Internet Explorer
- Activación de Navegación Privada: Sin cookies, historia, formularios
  - Chrome: **Ctrl + Shift + N**
  - Firefox, Edge, Internet Explorer: **Ctrl + Shift + P**



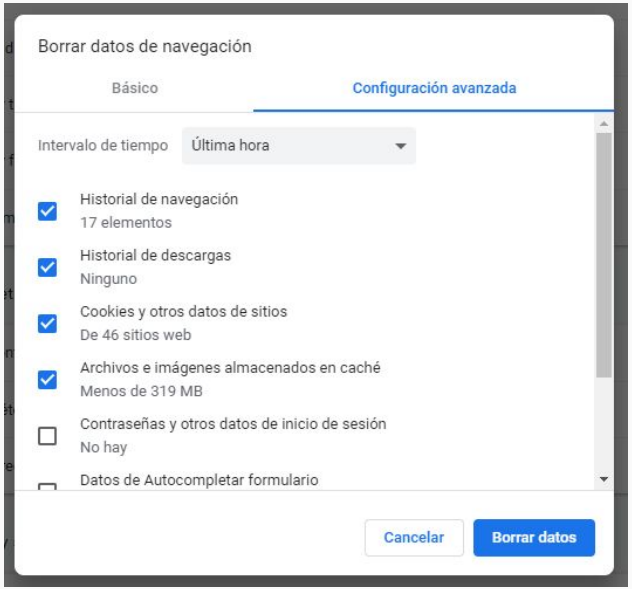


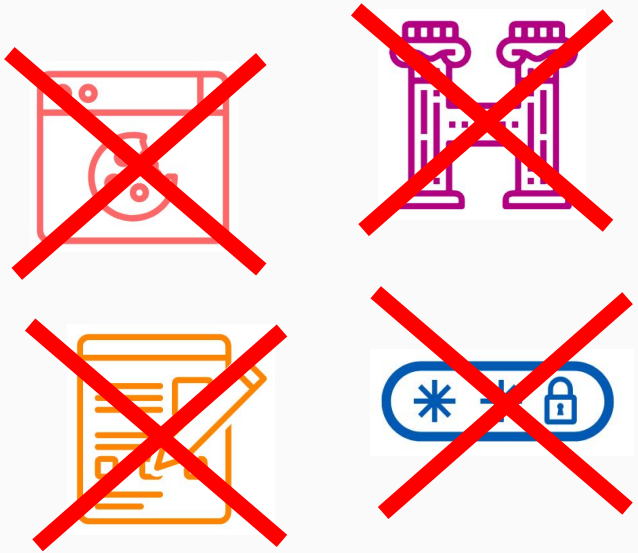




Buenas Prácticas: Limpieza de datos del browser

- Limpieza de Datos: Borrar selectivamente cookies, historia, formularios, password
  - Chrome, Firefox, Edge, Internet Explorer: **Ctrl + Shift + Supr**





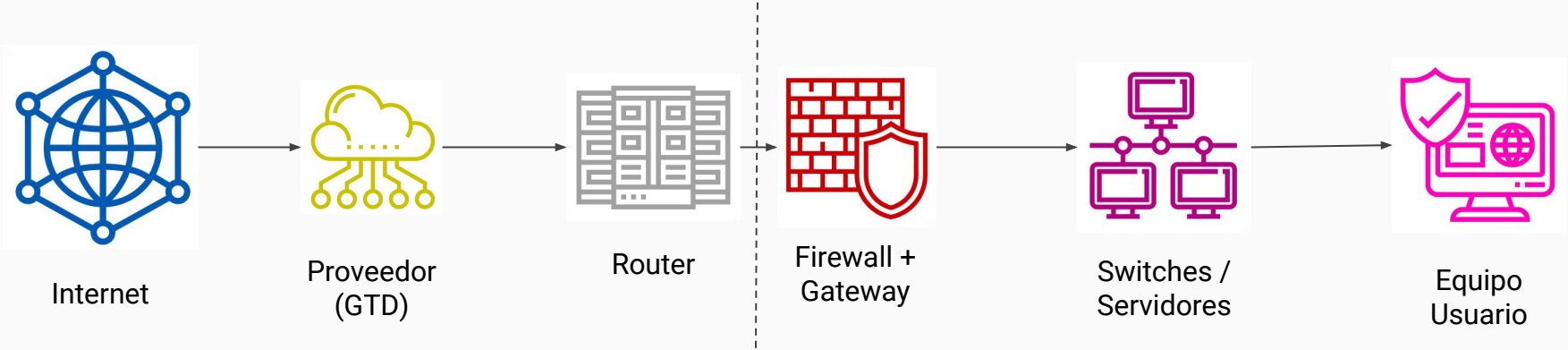
Buenas Prácticas: Misceláneas

Otras buenas prácticas:

- Mantener el software actualizado
- Bloquear equipo al dejarlo desatendido con ⊞ **+ L**
- Evitar redes públicas wifi desconocidas
- Solicitar privacidad al ingresar contraseñas; y asimismo, respetar el espacio de otros cuando ingresan contraseñas
- Respalde sus datos frecuente% → Google Drive
- Proteja su información sensible
- **¡No ejecute ni abra archivos desconocidos!**

Seguridad en **Conpax**

- **TIC**: Esquema simplificado de interconectividad



- **Legal**: Capítulo 25 Reglamento Interno (artículo 94)
  - Usar antivirus y comunicar sus alertas
  - Utilizar sólo los accesos que le fueron permitidos
  - Proteger la información en privacidad e integridad
  - Mantener confidencialidad y comunicar cualquier brecha de seguridad
  - Solo utilizar equipos, medios y software autorizados por la organización

Fin

¡Muchas gracias!

¿Dudas, comentarios, observaciones?