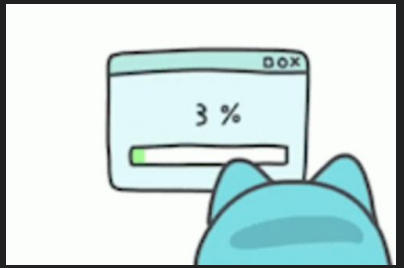
# De problemas y soluciones

CCESTE

# Tantas cosas que pueden fallar

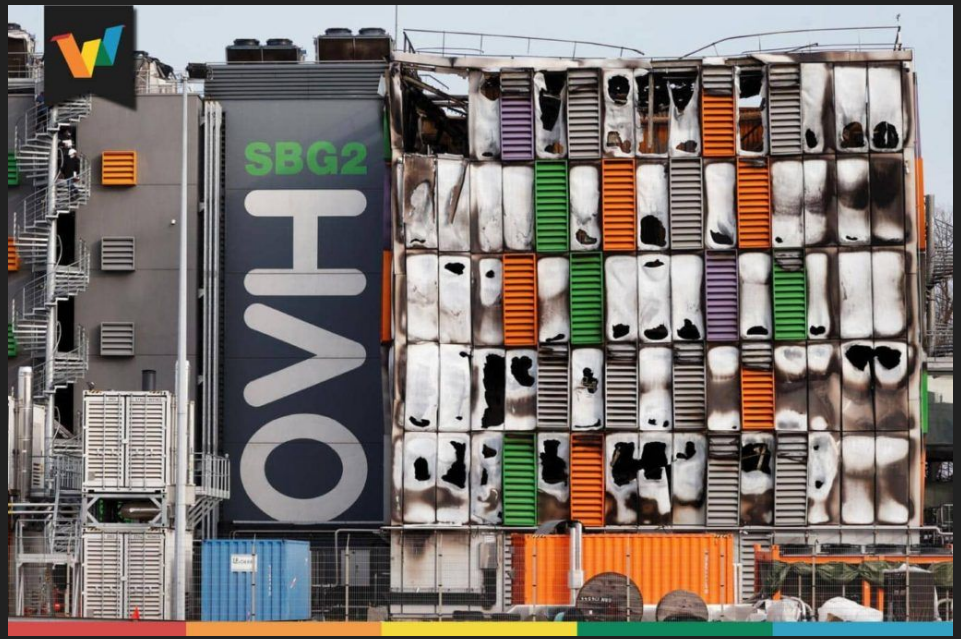
- Sistemas externos
- Sistemas internos
- Equipos de usuario
- Hardware de servidores
- Baremetal, VPS, instancias, DB administradas
- Redes corporativas
- Redes de servicios
- Sistemas eléctricos
- CCTV
- ***Impresoras***



# Tipos de problemas según el CCE y ponele que CompTIA

- Degradado
  - Funca, pero lento, no escala, pero se pueden completar las operaciones
  - *AFIP o Homebanking un lunes 8am*
- Con errores
  - Funca, puede estar degradado, pero algunas operaciones dan errores
  - *Terminal PoS rebotó la tarjeta, MercadoPago / Modo, tuviste que escanear el QR de nuevo*
- Corrupto
  - Funciona, pero las operaciones están corruptas, puede incluir las otras
  - *Te debitaron $20K en vez de $2000. Mandaste a imprimir y sale en blanco*
- Caído
  - *Inoperable, no responde*
  - *La compu no prende, el cajero fuera de servicio, la web con error 500*
- Comprometido
  - Se te metieron, alguien o algo 😵. Los datos y los equipos ya no son confiables
  - *Ransomware, fotos de la CC o DNI, te crackearon el pass, te abrieron la compu y se llevaron el disco*
- FUBAR - fucked up beyond all repair
  - Se prendió fuego, se inundó, se rompió y el fabricante quebró en el ‘84

# FUBAR




**Octave Klaba** @olesovhcom · Mar 9, 2021

We have a major incident on SBG2. The fire declared in the building. Firefighters were immediately on the scene but could not control the fire in SBG2. The whole site has been isolated which impacts all services in SGB1-4. We recommend to activate your Disaster Recovery Plan.

377 3,471 4,651

**Octave Klaba** @olesovhcom · Mar 10, 2021

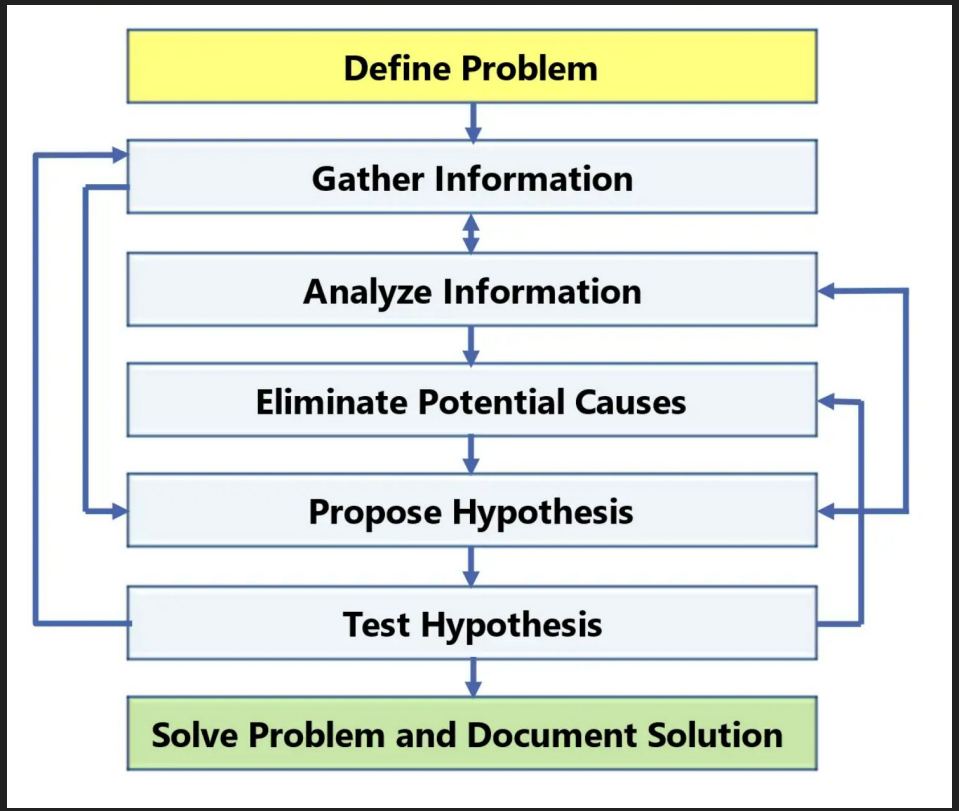
Update 5:20pm. Everybody is safe.
Fire destroyed SBG2. A part of SBG1 is destroyed. Firefighters are protecting SBG3. no impact SBG4.

124 620 1,646

**Octave Klaba** @olesovhcom · Mar 10, 2021

Update 7:20am
Fire is over. Firefighters continue to cool the buildings with the water. We don't have the access to the site. That is why SBG1, SBG3, SBG4 won't be restarted today.

# Procedimiento estándar




Qué es lo que pasa?
A quiénes o a qué afecta?
Desde cuando?

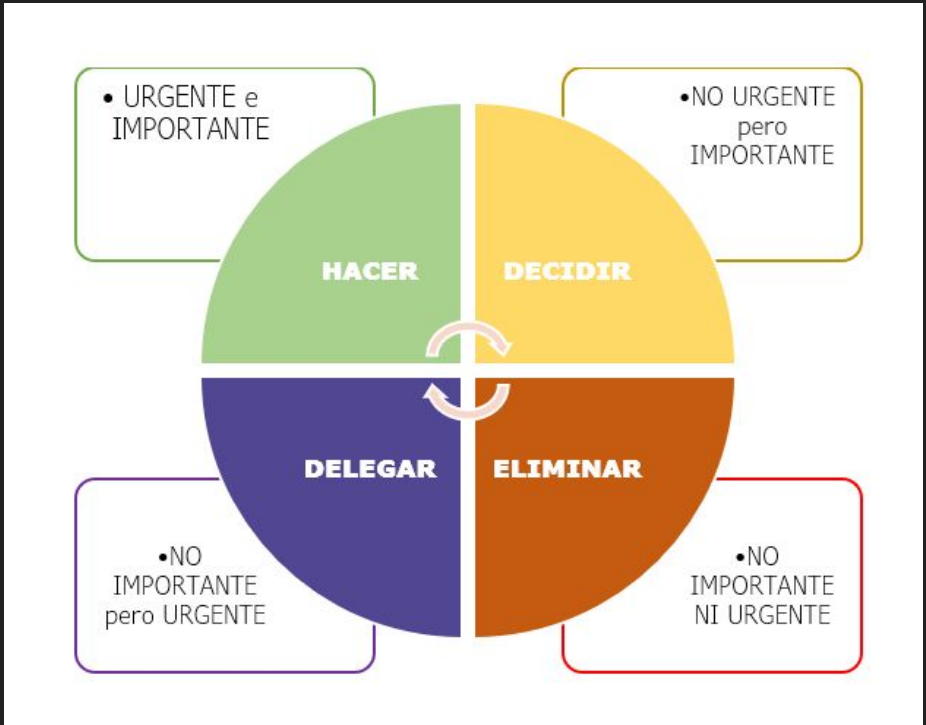
Que se ha modificado desde ese momento - y que puede afectar? *Tenes q saberlo*

Que se ha cambiado y que *creemos* que no puede afectar? *Tenes q saberlo*

Dónde está documentado esto?
Está documentado? *Hay que documentarlo*
Está monitoreado? *Hay que monitorearlo*

En base a la info anterior, aplicar las soluciones que correspondan, y documentar el evento

# Evaluar qué clase de kilombo es




Si te reclamaron por un problema, tenes que decidir ***vos*** por el usuario y darle la prioridad que corresponda.

Algunos ni siquiera te corresponden, si el SQL está caído, es tu asunto… o quizá del DBA

Si la cafetera no cafetea, *hace valer tu tiempo*

# Sistemas Externos  - Sin contrato

AFIP

Bancos

APIs

DNS

Plataformas

- Youtube
- WhatsApp
- Amazon

Tren de tickets y reclamos

Difícil de aislar a un sector

No se sabe el ETR (Estimated Time to Restoration)

No hay a quién llamar

Googlear, statuspage.io o chequear r/sysadmin es tiempo

Favor es convidar un mate, empujar un auto a un desconocido

No menos de $5 por esto, ni de favor, ni gauchada, sos un profesional

# Sistemas Externos  - Con contrato

SaaS - de lo que venga

- CRM
- Billing
- CloudFlare
- Teams - Workspace - Slack

APIs

Hosting / Colocation / Redes de proveedores

Acceso remoto - Teamviewer, Anydesk, ConnectWise

Reclamos puntuales sobre el sistema

Afecta sólo a algunos

*Quizá* hay ETR de resolución

*Debería* haber un contacto a quién llamar

***Pagaron la licencia????***

No menos de $10/h por levantar el teléfono o mandar un mail

Tiene valor saber a quien llamar, saber a quien preguntar, si hay un contrato en el medio estas poniendo tu nombre en el medio también

# Equipos de usuario

Monitor no prende

Compu no arranca

Periféricos no funcionan

Internet no anda

Cafetera no cafetea

***La impresora no es hardware de usuario,*** y siempre va a convenir tercerizar a alguien eso

Importante, no urgente

Reemplazar primero, reparar después

Reemplazar es quizá mover a la persona a otro escritorio y no reemplazar la compu

# Hardware de servidores y redes

Roturas en PSU, discos, fans, placas

BIOS corrupta

iDrac / iLO sin licencia

Controladora RAID muerta o pronta a fallar

Temperatura

Puertos rotos / quemados

Cables fallados, transcievers muertos

Equipo fuera de garantía y sin soporte

Importante, y quizá urgente, siempre preferir el failover al downtime

Reemplazar siempre, reparar nunca, dormí en paz

# Baremetal, VPS, instancias, DB administradas

Mantenimiento programado y no te enteraste

Te encerraste solo via firewall

Te hackearon

Destruiste la instancia

Dropeaste la DB

El proveedor fue comprometido

No hay documentación ni contratos al día

Que se ha modificado desde ese momento - y que puede afectar?
Tenés que saberlo

Que se ha cambiado y que creemos que no puede afectar?
Tenés que saberlo

Está documentado?
Hay que documentarlo

Está monitoreado?
Hay que monitorearlo - y te habrías ahorrado los pasos anteriores

# Redes corporativas

VPN no conecta

Servidor de archivos / RDP / muerto, caído

Archivos rotos, perdidos

**No hay backups**

- *y hay backup offline ????*

CRM, Billing, Sistemas sin soporte

AV muerto

- Licencia? $$ o confiá en defender - no AV trucho

Ransomware

- May the force be with you, godspeed, a los backups

No hay documentación ni contratos al dia

Si es tu laburo dia a dia, ***tranquilo y te tomás un mate que nadie te va a pagar extras por andar corriendo***

Si es consulting, no menos de $20/h por esto si es cliente regular - porque ya deberías tener documentado y monitoreado todo - actuá como profesional

No menos de $30 si es cliente nuevo en emergencia, y le ofreces el discovery, documentación, recomendaciones y monitoreo al rate estándar de arriba

# Redes de servicios

Sitio caído por falla física

Cliente caído por falla autogenerada

Averia masiva

No hay documentación

Bugs en equipos de red

Upstreams con problemas

No hay backups

No hay logs

Transporte de proveedor caído / degradado

Si es tu laburo dia a dia, ***tranquilo y te tomás un mate que nadie te va a pagar extras por andar corriendo***

Si es consulting, no menos de $30/h por esto si es cliente regular - porque ya deberías tener documentado y monitoreado todo - actuá como profesional

No menos de $40 si es cliente nuevo en emergencia, y le ofreces el discovery, documentación, recomendaciones y monitoreo al rate estándar de arriba

# Sistemas eléctricos

UPS

Zapatilla perdida debajo de un escritorio

Generadores, tableros, 220VAC

- *para eso está el electricista, cuidate*

Alarmas

- *llamá al que puso la alarma*

Control de acceso

- *si es tu sala de comunicaciones.. entendé cómo funciona, no te querés quedar afuera*
- *no solo es digital, es también tener copia de las llaves y saber donde están*

Si es tu laburo dia a dia, ***tranquilo y te tomás un mate que nadie te va a pagar extras por andar corriendo - pero la electricidad te puede joder muchas otras cosas, mas vale prevenir que curar***

Si es consulting, no menos de $10/h por esto Relevás lo que entiendas, llamá al electricista y que presupueste. Y vos cobrá por tu gestión.

Cliente nuevo en emergencia, llamá al electricista de confianza, que arregle el rate el.

# CCTV

Cámara muerta

Sin espacio para grabaciones

Sin soporte APP remota

DVR chino dudosa procedencia

Nadie sabe las claves y todos acceden

No hay documentación

# Impresoras

Driver jodiendo o desactualizado

Papel atorado

Mecanismo fallado

***Que lo maneje una tercera parte, lo van a hacer mucho mejor que vos***

Bueno bueno pero como cobro?

# Rates en consulting

Decidí un $ por hora (si, por hora).

No te parece? Ofrece un pack de 10hs prepagas, y uno de 25 y le cobrás solo 20

Emergencias es mínimo 2hs, 1.5x el rate

Fuera de horario es mínimo 2hs, 1.5x el rate

Cliente tiene un contacto técnico a la altura adentro

- fraccioná en ¼ de hora
- caso contario, mínimo ½ hora

Fracción es si tuviste que dejar lo que estabas haciendo para darle bola. “Manos sucias”

*Al cliente no le gusta que busque a otro, viví tranquilo que no todo es plata y somos un montón en este mundo*

# El know how

Viste que ahora le dicen así 😂

Que algo te parezca difícil, no quiere decir que nadie más sea capaz de lograrlo.

- Dijo Marco Aurelio en Gladiador

# Linux

- `ps faux`
- `htop`
- `free -h`
- `dmesg`
- `df -h`
- `who`
- `/var/log/*`
- `ss`
- `ip link show`
- `ip addr show`
- `ip route show`
- `iptables -L`
- `systemctl xxx status`
- `uptime`

Como estamos de:

- procesos, % CPU, memoria
- logs raros?
- espacio en disco?
- quien está adentro?
- logs en detalle
- puertos y sockets activos
- direcciones IP, interfaces, rutas
- firewall
- estado del servicio en cuestión
- se reinició?

Tenemos idea de como se ve cuando está todo ok?

# Windows

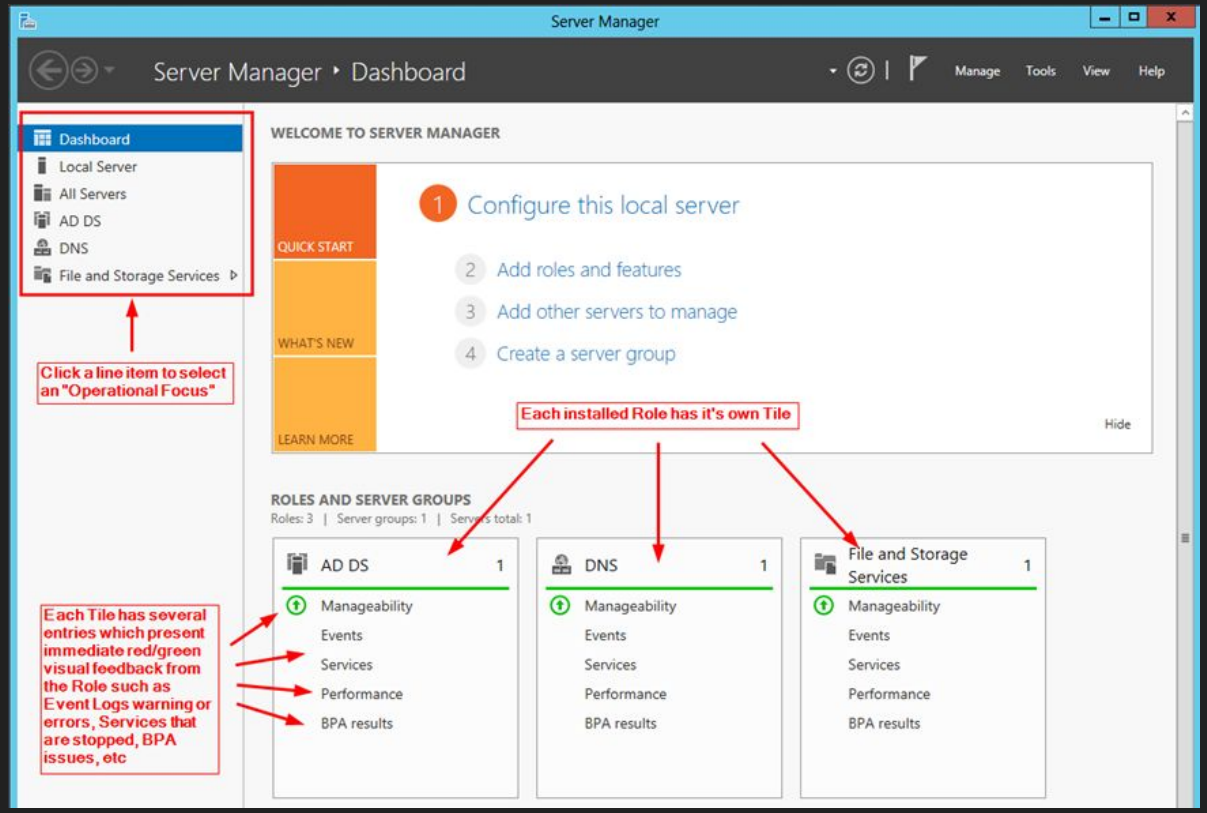
- Task manager - Ctrl+Shift+Esc
- Rendimiento
- Visor de eventos
- Server manager
- Servicios andando
- netstat
- Firewall de windows
- **Drivers de la VM !**
- Nirsoft *mi buen amigo toda la vuelta vamo a dar ♪♬*
- Sysinternals

Como estamos de:

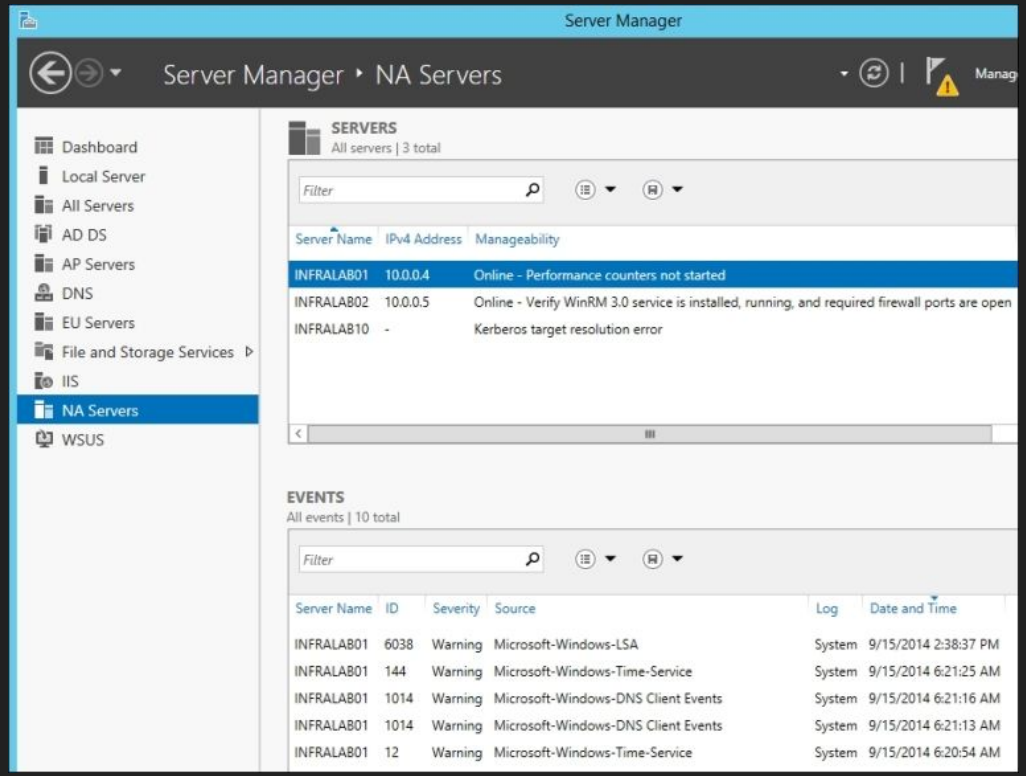
- procesos, % CPU, memoria
- espacio en disco?
- quien está adentro?
- logs raros?
- logs en detalle
- puertos y sockets activos
- direcciones IP, interfaces, rutas
- firewall
- estado del servicio en cuestión

Tenemos idea de como se ve cuando está todo ok?

# Windows

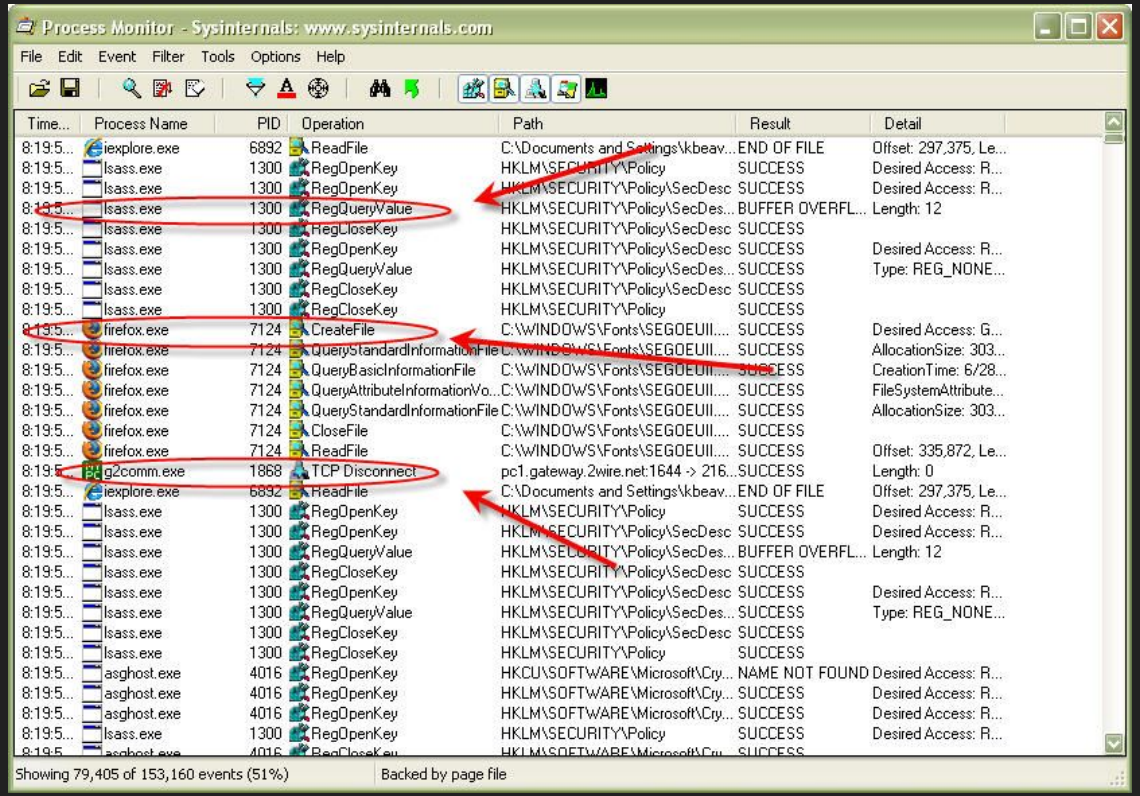

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
Click a line item to select an "Operational Focus"
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
Hide
Each installed Role has it's own Tile
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
AD DS 1
Manageability
Events
Services
Performance
BPA results
DNS 1
Manageability
Events
Services
Performance
BPA results
File and Storage Services 1
Manageability
Events
Services
Performance
BPA results
Each Tile has several entries which present immediate red/green visual feedback from the Role such as Event Logs warning or errors, Services that are stopped, BPA issues, etc

# Windows


Server Manager
Server Manager ‣ NA Servers
Manag
Dashboard
Local Server
All Servers
AD DS
AP Servers
DNS
EU Servers
File and Storage Services
IIS
NA Servers
WSUS
SERVERS
All servers | 3 total
Filter
Server Name IPv4 Address Manageability
INFRALAB01 10.0.0.4 Online - Performance counters not started
INFRALAB02 10.0.0.5 Online - Verify WinRM 3.0 service is installed, running, and required firewall ports are open
INFRALAB10 - Kerberos target resolution error
EVENTS
All events | 10 total
Filter
Server Name ID Severity Source Log Date and Time
INFRALAB01 6038 Warning Microsoft-Windows-LSA System 9/15/2014 2:38:37 PM
INFRALAB01 144 Warning Microsoft-Windows-Time-Service System 9/15/2014 6:21:25 AM
INFRALAB01 1014 Warning Microsoft-Windows-DNS Client Events System 9/15/2014 6:21:16 AM
INFRALAB01 1014 Warning Microsoft-Windows-DNS Client Events System 9/15/2014 6:21:13 AM
INFRALAB01 12 Warning Microsoft-Windows-Time-Service System 9/15/2014 6:20:54 AM

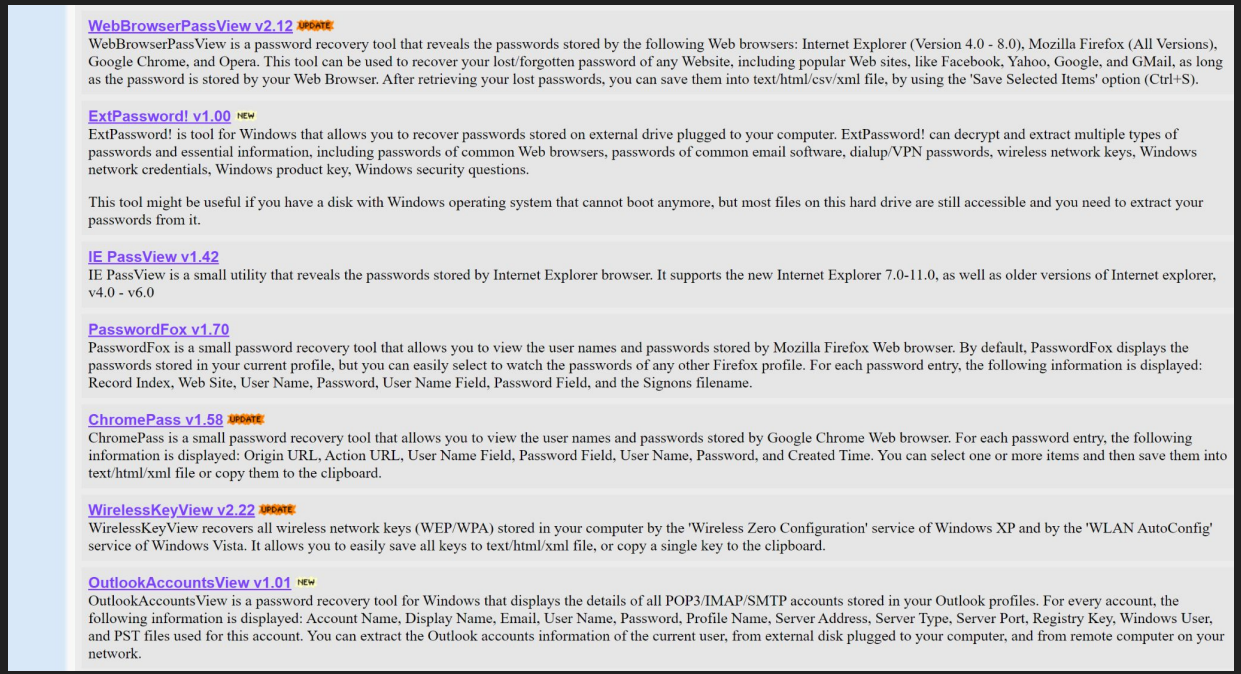
# Sysinternals

https://learn.microsoft.com/es-es/sysinternals/downloads/?source=recommendations



# Nirsoft

https://www.nirsoft.net/utils/index.html



**WebBrowserPassView v2.12** UPDATE
WebBrowserPassView is a password recovery tool that reveals the passwords stored by the following Web browsers: Internet Explorer (Version 4.0 - 8.0), Mozilla Firefox (All Versions), Google Chrome, and Opera. This tool can be used to recover your lost/forgotten password of any Website, including popular Web sites, like Facebook, Yahoo, Google, and GMail, as long as the password is stored by your Web Browser. After retrieving your lost passwords, you can save them into text/html/csv/xml file, by using the 'Save Selected Items' option (Ctrl+S).

**ExtPassword! v1.00** NEW
ExtPassword! is tool for Windows that allows you to recover passwords stored on external drive plugged to your computer. ExtPassword! can decrypt and extract multiple types of passwords and essential information, including passwords of common Web browsers, passwords of common email software, dialup/VPN passwords, wireless network keys, Windows network credentials, Windows product key, Windows security questions.

This tool might be useful if you have a disk with Windows operating system that cannot boot anymore, but most files on this hard drive are still accessible and you need to extract your passwords from it.

**IE PassView v1.42**
IE PassView is a small utility that reveals the passwords stored by Internet Explorer browser. It supports the new Internet Explorer 7.0-11.0, as well as older versions of Internet explorer, v4.0 - v6.0

**PasswordFox v1.70**
PasswordFox is a small password recovery tool that allows you to view the user names and passwords stored by Mozilla Firefox Web browser. By default, PasswordFox displays the passwords stored in your current profile, but you can easily select to watch the passwords of any other Firefox profile. For each password entry, the following information is displayed: Record Index, Web Site, User Name, Password, User Name Field, Password Field, and the Signons filename.

**ChromePass v1.58** UPDATE
ChromePass is a small password recovery tool that allows you to view the user names and passwords stored by Google Chrome Web browser. For each password entry, the following information is displayed: Origin URL, Action URL, User Name Field, Password Field, User Name, Password, and Created Time. You can select one or more items and then save them into text/html/xml file or copy them to the clipboard.

**WirelessKeyView v2.22** UPDATE
WirelessKeyView recovers all wireless network keys (WEP/WPA) stored in your computer by the 'Wireless Zero Configuration' service of Windows XP and by the 'WLAN AutoConfig' service of Windows Vista. It allows you to easily save all keys to text/html/xml file, or copy a single key to the clipboard.

**OutlookAccountsView v1.01** NEW
OutlookAccountsView is a password recovery tool for Windows that displays the details of all POP3/IMAP/SMTP accounts stored in your Outlook profiles. For every account, the following information is displayed: Account Name, Display Name, Email, User Name, Password, Profile Name, Server Address, Server Type, Server Port, Registry Key, Windows User, and PST files used for this account. You can extract the Outlook accounts information of the current user, from external disk plugged to your computer, and from remote computer on your network.

# Migral compuesto

Sysinternals y Nirsoft

Veeam para tus VM o Nakivo, lo que alcanze el $$

Veeam para Office365 y Workspace

Un destino ***offsite*** para tus backups

Los backups obviamente, Bacula, Duplicati, Borg, Veeam. Si tiene autoservicio mejor

Documentación ***offline*** en tu compu

Un reparador de PST

Par de USB W10, W11, eviten W7 en lo posible

lucid.app o diagrams.net

# Redes, de tu lado

- `ping 1.1.1.1` *asi rapidito*
- `ping -l 1472 -f 1.1.1.1` *asi mas largo*
- `tracert -w 1 -d 1.1.1.1` *EN WIN*
- `traceroute -w 1 -n 1.1.1.1` *EN NIX*
- `nslookup google.com 1.1.1.1`
- `arp -a`
-
- `ipconfig /renew` en win
- `dhclient XX` en linux
-
- `route print` en win
- `ip ro show` en linux

Como estamos de:

- ICMP
- MTU de 1500
- camino para afuera
- resolución DNS
- resolución ARP
- cliente DHCP
- rutas que no debieran estar ? una vpn que quedó activa y no viste?

Tenemos idea de como se ve cuando está todo ok?

# Redes, de tu lado

- `ping 1.1.1.1` *asi rapidito*
- `ping -l 1472 -f 1.1.1.1` *asi mas largo*
- `tracert -w 1 -d 1.1.1.1` *EN WIN*
- `traceroute -w 1 -n 1.1.1.1` *EN NIX*
- `nslookup google.com 1.1.1.1`
- `arp -a`
-
- `ipconfig /renew` en win
- `dhclient XX` en linux
-
- `route print` en win
- `ip ro show` en linux

Como estamos de:

- ICMP
- MTU de 1500
- camino para afuera
- resolución DNS
- resolución ARP
- cliente DHCP
- rutas que no debieran estar ? una vpn que quedó activa y no viste?

Tenemos idea de como se ve cuando está todo ok?

# Redes, del otro lado - Cisco

- `sh inte desc`
- `sh inte te1/1`
- `sh ip inte br`
- `sh ipv6 inte br`
- `sh ip os neigh`
- `sh ip os inte`
- `sh ip bgp s2umm`
- `sh route`
- `ping x.x.x.x size 1500`
- `traceroute x.x.x.x numeric`
- `sh log`
- **`1-800-TAC !`**

Como estamos de:

- interfaces activas
- niveles de potencia optica, CRC, drops, MTU
- direcciones ip4 e ip6
- vecinos OSPF
- peers BGP
- ICMP
- camino para afuera
- el log

Tenemos idea de como se ve cuando está todo ok?

# Redes, del otro lado - Juniper

- `show inte desc`
- `show inte xe-0/0/0 diag`
- `show ospf neigh`
- `show bgp summ`
- `show route`
- `ping x.x.x.x size 1500`
- `traceroute x.x.x.x num`
- `sh log messages`
- `supportportal.juniper.com`
- `r/networking`
- **`1-800-TAC !`**

Como estamos de:

- interfaces activas
- niveles de potencia optica, CRC, drops, MTU
- direcciones ip4 e ip6
- vecinos OSPF
- peers BGP
- ICMP
- camino para afuera
- el log

Tenemos idea de como se ve cuando está todo ok?

# Redes, del otro lado - De cualquier lado

Como estamos de:

- interfaces activas
- niveles de potencia optica, CRC, drops, MTU
- direcciones ip4 e ip6
- vecinos OSPF
- peers BGP
- ICMP
- camino para afuera
- el log
- wireshark al rescate

Configuration guide, offline en tu compu

Tenemos idea de como se ve cuando está todo ok?

Todo tiene arreglo,
salvo el ransomware

Cuidá tus backups