ASOCIACIÓN DE PROFESIONALES EN DESARROLLO DE LA ORGANIZACIÓN

APDO

## Charla de Divulgación

# Ciberseguridad en la Empresa


Perito IT

***"No obtiene justicia quien posee la verdad sino aquel que mejor la evidencia y la demuestra"***

***- Rafael López -***

Barcelona, 30 de enero de 2020

# Ciberseguridad en la Empresa


## *Rafael López Rivera*

***Perito Judicial Informático y Tecnológico***

*Vicepresidente de la ACPJT*
*Fundador de ANCITE y APTAN*
*Miembro ASPERTIC y STOP VdG DIGITAL*

Perito IT

**www.peritoit.com**

# INTRODUCCIÓN Y REFERENTE

# Ciberseguridad en la Empresa

## El referente: INCIBE

INSTITUTO NACIONAL DE CIBERSEGURIDAD

**INCIBE es el Instituto Nacional de Ciberseguridad de España**
**www.incibe.es**

- **Es la entidad gubernamental para el desarrollo de la ciberseguridad** liderando actuaciones para la Ciberseguridad a nivel nacional e internacional.

- **Opera el CERT (Computer Emergency Response Team) de Seguridad e Industria** para la detección y alerta temprana de nuevas amenazas con análisis y respuesta a incidentes de seguridad y la lucha contra ciberdelitos.

- **Diseña medidas preventivas** para atender a las necesidades de Ciberseguridad la Sociedad en General.

# Ciberseguridad en la Empresa

## Decálogo de Ciberseguridad para las Empresas


### DECÁLOGO PARA LA EMPRESA SEGURA SEGÚN INCIBE

### LO BÁSICO E IMPRESCINDIBLE

1. Política y Normativa
2. Control del Acceso
3. Copias de Seguridad
4. Protección Antimalware
5. Actualizaciones de Software
6. Seguridad en la red

### MEDIDAS DE REFUERZO Y MEJORA

7. Información en Tránsito
8. Gestión de Soporte
9. Registro de la Actividad
10. Continuidad del Negocio

**Enlace Web al Documento:**

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

# LO BÁSICO E IMPRESCINDIBLE

# 1 . POLÍTICA Y NORMATIVA

## El Compromiso con la Seguridad se define:

A) Por medio de una **Política de Seguridad** que defina cómo se va a abordar la seguridad para cada uno de los diferentes aspectos y elementos relevantes de la empresa.

B) Soportada por el desarrollo de **Normativas y Procedimientos** que recogen las obligaciones a la que están sujetos los Stakeholders y los afectados.

# Ciberseguridad en la Empresa

## Plan Director de Ciberseguridad – Hoja de Ruta

**Especialista Informático**

**AS IS**

**Análisis de la situación actual**: Políticas, normativas, procedimientos, equipamiento, canales, dispositivos, personal, riesgos inherentes, etc.

ISO 27002

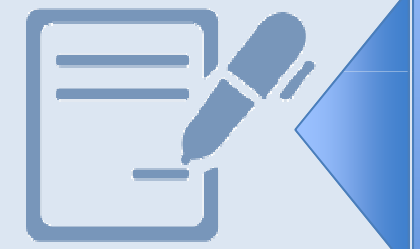
**TO BE**

**Determinar el nivel de Seguridad que se desea alcanzar en la empresa** en función de sus características: sector y negocio, tipo de información manejada, objetivos empresariales, exigencias del mercado y normativa.

**PLAN DIRECTOR DE CIBERSEGURIDAD - HOJA DE RUTA PERSONALIZADA -**

# Ciberseguridad en la Empresa

## Políticas a implementar (Mínimas deseables)



**POLÍTICAS**

- Política de aplicaciones permitidas y de uso de software legal.
- Política de Uso de Medios de la Empresa (dispositivos PC, Smartphone, tabletas, etc.).
- Política de usos de medios personales (BYOD)
- Política de accesos externos (Wifi's, VPN. Etc.) y Política de Contraseñas.
- Política de Almacenamiento de la información (red corporativa, copias de seguridad, almacenamiento local y en la nube, etc.)
- Política de borrado y destrucción segura de la información electrónica.
- Políticas de uso de Correo Electrónico.
- Política de Instalación y Actualizaciones.

# Ciberseguridad en la Empresa

## Cumplimientos Legales que afectan a los Sistemas

**LEGISLACIÓN APLICABLE A SISTEMAS INFORMÁTICOS**

**RGPD – Reglamento Europeo 679/2016 de Protección Datos**
**LOPDGDD – LO 3/2018 Protección de Datos y Garantías de Derechos digitales**
Vela por la seguridad de los datos y ficheros de carácter personal.
Implementa medidas de seguridad para evitar el acceso no autorizado a dicha información.

**LPI – RDL 1/996. Ley de la Propiedad Intelectual**
► Protege el conocimiento, el Know-How y la información empresarial.
► Vigilancia de la utilización de software no licenciado o copias piratas de software en la empresa.

**LSSICE – Ley 34/2002 Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.**
Afecta a empresas dedicadas a actividades económicas por medio de servicios online o de business e-commerce.

► **Acuerdos de Responsabilidad de los Proveedores.**
► **Acuerdos de Confidencialidad con los Empleados.**

# 2 . CONTROL DE ACCESO

## EL ESCENARIO DE LOS ACCESOS ES GLOBAL

- **SITUACIÓN y LOCALIZACION de los elementos de almacenamiento y repositorios** de la información tanto internos (otras sedes o localizaciones remotas, en la nube) como externos (Externalización de los servidores y de Aplicativos).

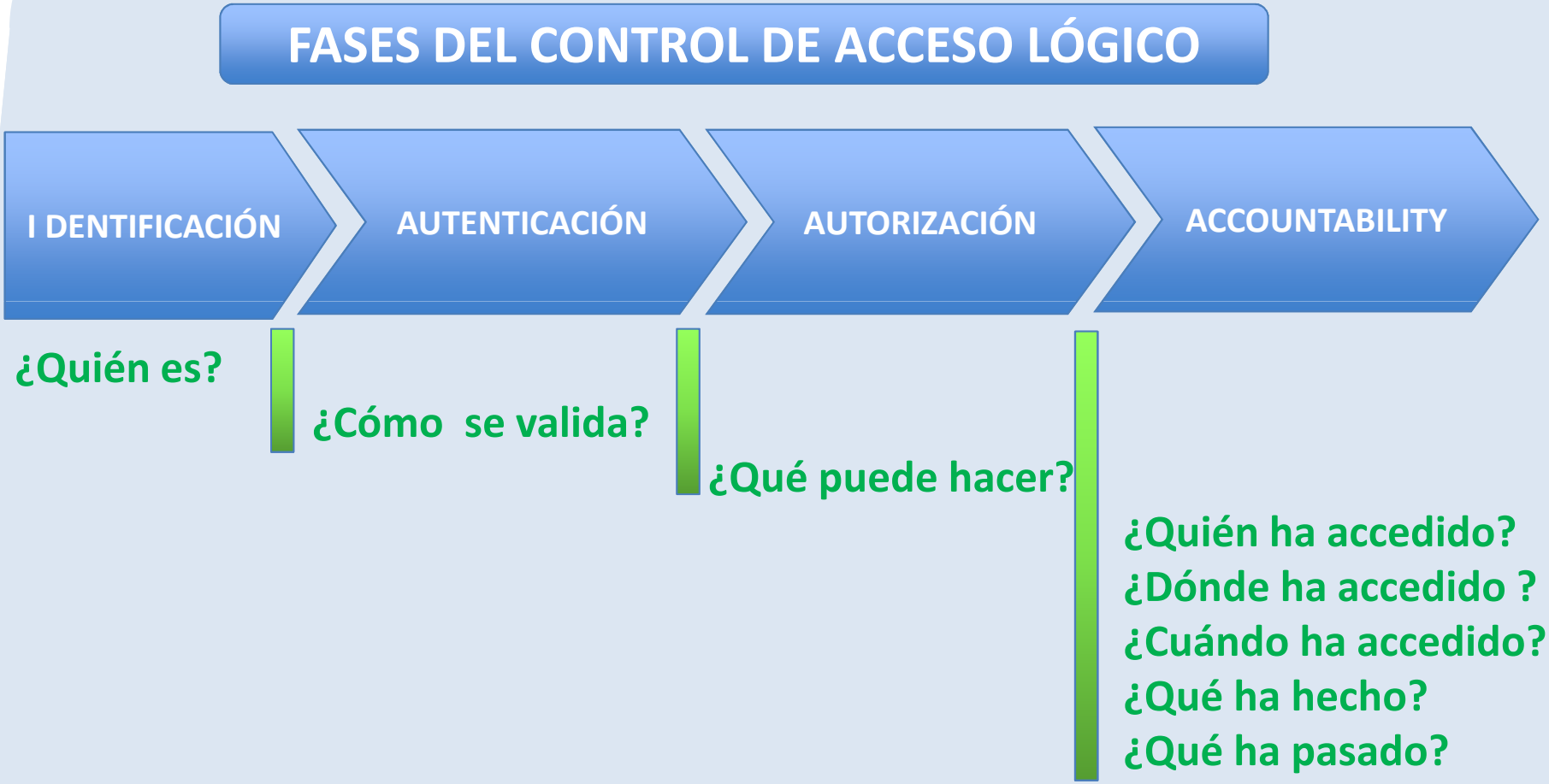
- **NECESIDADES DE ACCESO, tanto internas como externas** por medio de accesos externos seguros (teletrabajo, oficina móvil, movilidad, sedes y centros, etc.).

- **CONEXIONES DISPOSITIVOS INALÁMBRICOS**.

- **DISPOSITIVOS AJENOS** (BYOD, red de invitados, proveedores de servicios IT)

# Ciberseguridad en la Empresa

## Fases del Control del Acceso Lógico



# 3 . COPIAS DE SEGURIDAD

## COPIAS DE SEGURIDAD

- **Las Copias o Backup de Seguridad es el elemento preventivo básico**, necesario e imprescindible que se ha de poseer para poder afrontar cualquier tipo de incidente de seguridad, bloqueo, daño o pérdida de información de la Organización y de los Sistemas.

- Las Copias de Seguridad **es el único elemento que puede llegar a permitir la restauración o restitución de un Sistema y de la totalidad de la información contenida** en los mismos tras un incidente de Seguridad.

- **La posible Continuidad del Negocio va a depender de la existencia, actualización, recuperación y operatividad efectiva real de las Copias de Seguridad.**

# Ciberseguridad en la Empresa

## Consideraciones de las Copias de Seguridad


**EL ALCANCE**

Se ha de determinar que información es básica a ser preservada, dónde se encuentra, dónde debe ser depositada por los sistemas y usuarios para ser preservada.

**TEMPORALIDAD**

- ► Cada cuánto tiempo es necesario realizar esta Copia de Seguridad para cada tipo de información.
- ► Cuántas copias se ha de preservar y de qué tipo incremental / diferencial / totales. Renovación/Historial.

**GESTIÓN**

- ► Quién tiene la responsabilidad de la gestión .
- ► Quién, cómo y cuándo se tiene acceso a la mismas.
- ► Qué información se guarda encriptada o reservada.
- ► Testeo de viabilidad de Restauración.

**MEDIOS FÍSICOS**

- ► Redundancia física e ubicación diferenciada.
- ► Equipos externos, servicios en nube, redes diferentes.

# Ciberseguridad en la Empresa

## Características de la Copia de Seguridad y del Proceso

**COPIAS DE SEGURIDAD**

**PROCESO DE RESTAURACIÓN**

**COPIA TOTAL**

Es necesario programar copias totales de la información a modo de puntos de restauración exhaustivos, globales y totales

**COPIAS INCREMENTALES O DIFERENCIALES**

En el supuesto que el volumen de información sea grande, se pueden programar copias parciales incluyendo solamente aquella información o ficheros de aquello que ha cambiado respecto a la última copia de seguridad .

**VALIDACIÓN DEL PROCESO DE RESTAURACIÓN**

► **Controles diarios** de la realización de las copias, de la existencia de espacio disponible y del éxito de la copia

► **Verificación periódica de restauración** de Copia total y con las Copias incrementales o diferenciales.

► **Verificación de la operatividad de información**.

# 4 . PROTECCIÓN ANTIVIRUS - ANTIMALWARES

## SOBRE LOS MALWARES

**MALWARE**, es la abreviatura de **Mal**icious Sort**ware.**

Dentro de este concepto de engloba todo tipo de programa o código informático de carácter netamente malicioso cuya función básicamente son:


► **Obtener ilícitamente información** o proporcionan información intrusivamente.

► **Bloquear o dañar un sistema**, causar un malfuncionamiento o **permitir el acceso al ciberdelincuente** o a sus procesos.

►**Aprovechar los recursos del sistemas** para su utilización en beneficio propio.

# Ciberseguridad en la Empresa

## Antivirus/Antimalware - Características

### Características de un Antivirus-Antimalware

► **Actualización Automática:** Debe actualizarse automáticamente con nuevos patrones y con la mayor periodicidad posible.

► **Análisis en Tiempo Real y Programado:** Debe ser capaz de realizar análisis en tiempo real de la actividad y se ha de poder programar para realizar análisis en profundidad de todo el dispositivo en periodos de inactividad del mismo.

► **Gestionar las Acciones:** Debe permitir la gestión de las acciones a ejecutar (cuarentena, borrado, etc.) ante un positivo.

► **Control de Páginas WEB, Correo Electrónico y Descargas:** Debe poder examinar en tiempo real amenazas que pudieran llegar por medio de las Comunicaciones de correo (Malware y Antispam) o de Internet (Malware y Antiphising). .

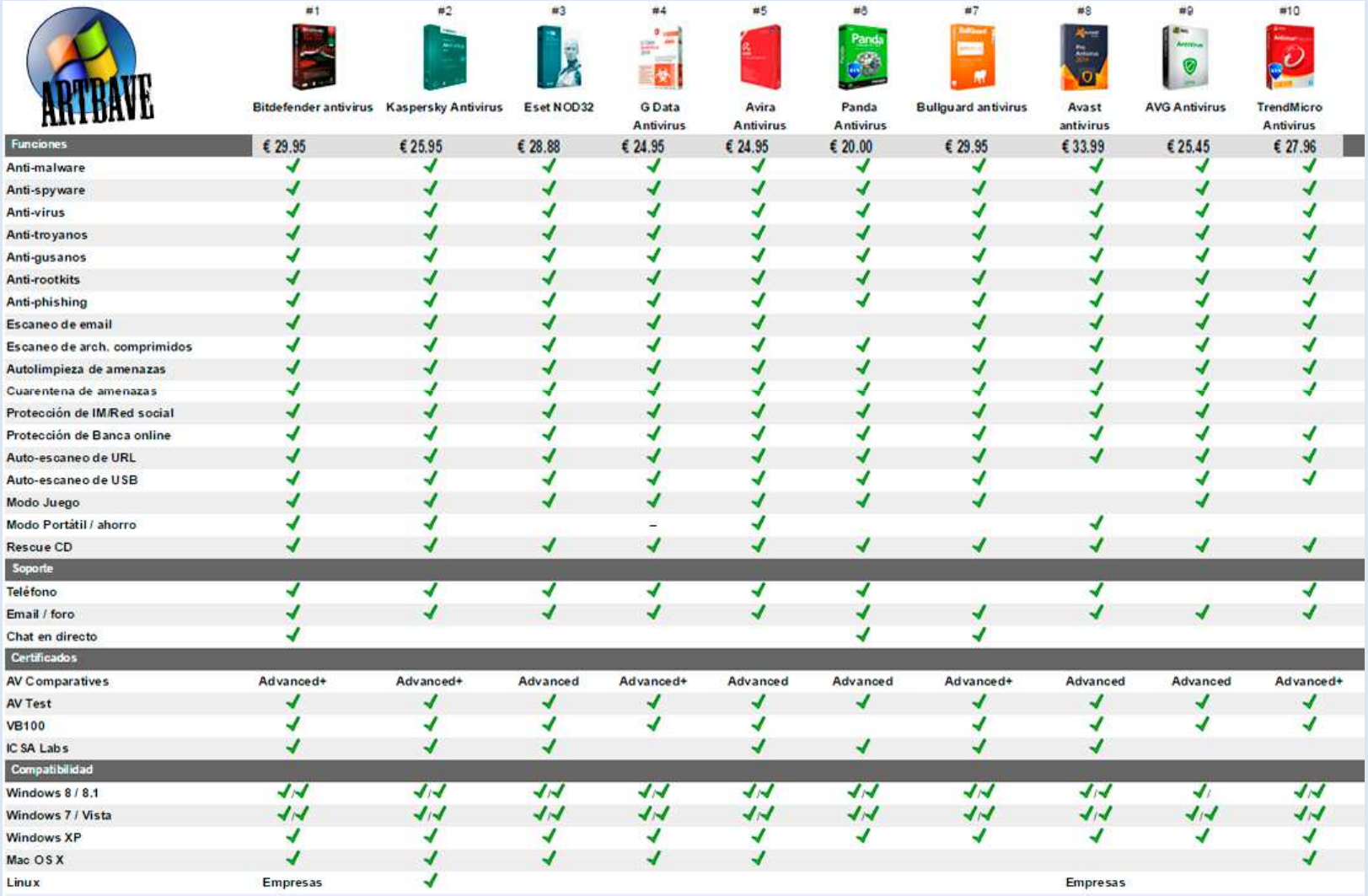
► **Funcionalidad de Sandbox:** Debe poseer un espacio seguro de cuarentena para ejecuciones dudosas o no fiables.

► **Funcionalidad de Firewall:** Debe poseer un cortafuegos para gestionar la autorizaciones de acceso.

► **Desinstalación por Administrador:** No debe ser posible desinstalarlo o inhabilitarlo con privilegios de usuario normal.

# Ciberseguridad en la Empresa

## Antivirus/Antimalware – De Pago



| | #1 Bitdefender antivirus | #2 Kaspersky Antivirus | #3 Eset NOD32 | #4 G Data Antivirus | #5 Avira Antivirus | #6 Panda Antivirus | #7 Bullguard antivirus | #8 Avast antivirus | #9 AVG Antivirus | #10 TrendMicro Antivirus |
|---|---|---|---|---|---|---|---|---|---|---|
| **Funciones** | € 29.95 | € 25.95 | € 28.88 | € 24.95 | € 24.95 | € 20.00 | € 29.95 | € 33.99 | € 25.45 | € 27.96 |
| Anti-malware | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Anti-spyware | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Anti-virus | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Anti-troyanos | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Anti-gusanos | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Anti-rootkits | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Anti-phishing | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Escaneo de email | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| Escaneo de arch. comprimidos | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Autolimpieza de amenazas | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cuarentena de amenazas | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Protección de IM/Red social | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Protección de Banca online | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Auto-escaneo de URL | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Auto-escaneo de USB | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Modo Juego | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Modo Portátil / ahorro | ✓ | ✓ | | - | ✓ | | | ✓ | | |
| Rescue CD | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Soporte** | | | | | | | | | | |
| Teléfono | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ |
| Email / foro | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Chat en directo | ✓ | | | | | ✓ | ✓ | | | |
| **Certificados** | | | | | | | | | | |
| AV Comparatives | Advanced+ | Advanced+ | Advanced | Advanced+ | Advanced | Advanced | Advanced+ | Advanced | Advanced | Advanced+ |
| AV Test | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| VB100 | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| IC SA Labs | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | |
| **Compatibilidad** | | | | | | | | | | |
| Windows 8 / 8.1 | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓ | ✓✓ |
| Windows 7 / Vista | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓✓ |
| Windows XP | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mac OS X | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | ✓ |
| Linux | Empresas | ✓ | | | | | | Empresas | | |

http://www.mejor-antivirus.es/comparativa-de-antivirus?p=baja&gclid=CjwKCAiAlfnUBRBQEiwAWpPA6Tz5b3fZlbWu1Oj6U1FWk0anJa4PAilSAbRkFqzUc4PHihxIJ98VpBoCMQcQAvD_BwE

# Ciberseguridad en la Empresa

## Antivirus/Antimalware – Gratuitos

| Nombre | Avast Free Antivirus 2016 | AVG AntiVirus Free (2016) | Panda Antivirus Gratis (2016) | Bitdefender Antivirus Free Edition (2014) | Check Point ZoneAlarm Free Antivirus + Firewall 2016 | Lavasoft Ad-Aware Free Antivirus + 11 | Malwarebytes Anti-Exploit gratuito | Qihoo 360 Total Security Essential | Comodo Antivirus 8 | FortiClient 5.0 |
|---|---|---|---|---|---|---|---|---|---|---|
| |  |  |  |  |  |  |  |  |  |  |
| El precio más bajo | Gratuito<br>Avast<br>SEE IT | Gratis<br>AVG Technologies<br>SEE IT | $ 0,00<br>MSRP | $ 0,00<br>MSRP | Gratis<br>ZoneAlarm<br>SEE IT | $ 0,00<br>MSRP | $ 0,00<br>MSRP | Libre<br>Amazon<br>SEE IT | $ 0,00<br>MSRP | $ 0,00<br>MSRP |
| Clasificaciones de los Editores | ●●●●◐ | ●●●●◐ | ●●●●◐ | ●●●●○ | ●●●●○ | ●●●●○ | ●●●●○ | ●●●◐○ | ●●●○○ | ●●●○○ |
| Número de Laboratorios de ensayo (más es mejor) | 6 | 4 | 3 | 3 | 1 | 2 | 0 | 3 | 2 | 4 |
| Agregada Lab Valoración (mayor es mejor) | 4 | 5 | 4 | 5 | N / A | 5 | N / A | 3 | 2 | 4 |
| PCMag Malware bloqueo (mayor es mejor) | 9.3 | 8.8 | 8.8 | 9.0 | 8.0 | 8.6 | N / A | 8.3 | 8.3 | 9.4 |
| PCMag malicioso URL Blocking (mayor es mejor) | 69% | 73% | 73% | N / A | 41% | 68% | N / A | 54% | 27% | 40% |
| On-Demand Malware Scan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ |
| Acceso on-Malware Scan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ |
| Sitio web Clasificación | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| Bloqueo de URL malicioso | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| Protección contra phishing | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ |
| La detección basada en comportamiento | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ |
| Bono: Análisis de vulnerabilidades | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

https://www.adslzone.net/2016/01/15/llega-kaspersky-free-antivirus-pero-que-mas-antivirus-gratuitos-tenemos-en-el-mercado/

# 5 . ACTUALIZACIONES DE SOFTWARE

## Actualizaciones de Software


► **Cualquier aplicación o solución software es susceptible de poseer vulnerabilidades.** Los fabricantes van publicando y distribuyendo actualizaciones (Parches) que resuelven estos problemas y mejoran el funcionamiento general del software.

► **Las actualizaciones son fuente de información de vulnerabilidades** que son estudiadas por los ciberdelincuentes para acceder a los sistemas y obtener el control de los mismos.

► **Los Ciberdelincuentes rastrean las redes en busca que equipos no actualizados** porque conocen las vulnerabilidades y debilidades y saben cómo "colarse" por medio de las mismas
Es una zona de la memoria, totalmente aislada del resto.

► **Es necesario poseer una base de datos de los activos** (CMDB-Configuration Management Database) tanto del software como del hardware con su configuración, características y nivel de actualización.

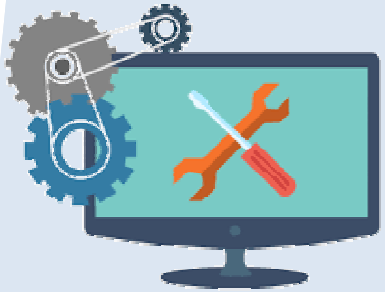
 

## Es necesario aplicar Actualizaciones de Software

Para mantener un nivel de Seguridad adecuados en los sistemas y aplicativos es necesario aplicar las actualizaciones (Update) y recomendaciones de los fabricantes lo antes posible para no dar tiempo a los Ciberdelincuentes a atacar nuestros equipos.

## Equipos o Sistemas especialmente afectados

***Hardware*: Servidores, ordenadores, elementos de red.**



***Software de Sistemas*:**

**Sistemas Operativos, gestores de Base de Datos, elementos de red, Correo Electrónico, Acceso Web, Antivirus/Antimalware, Navegadores.**

***Software de Usuario Final*:**

**Gestores de Contenido CMS (Wordpress, Joomla, Drupal)**
**Aplicativos de propósito (Ofimática-Contabilidad-ERP's) .**

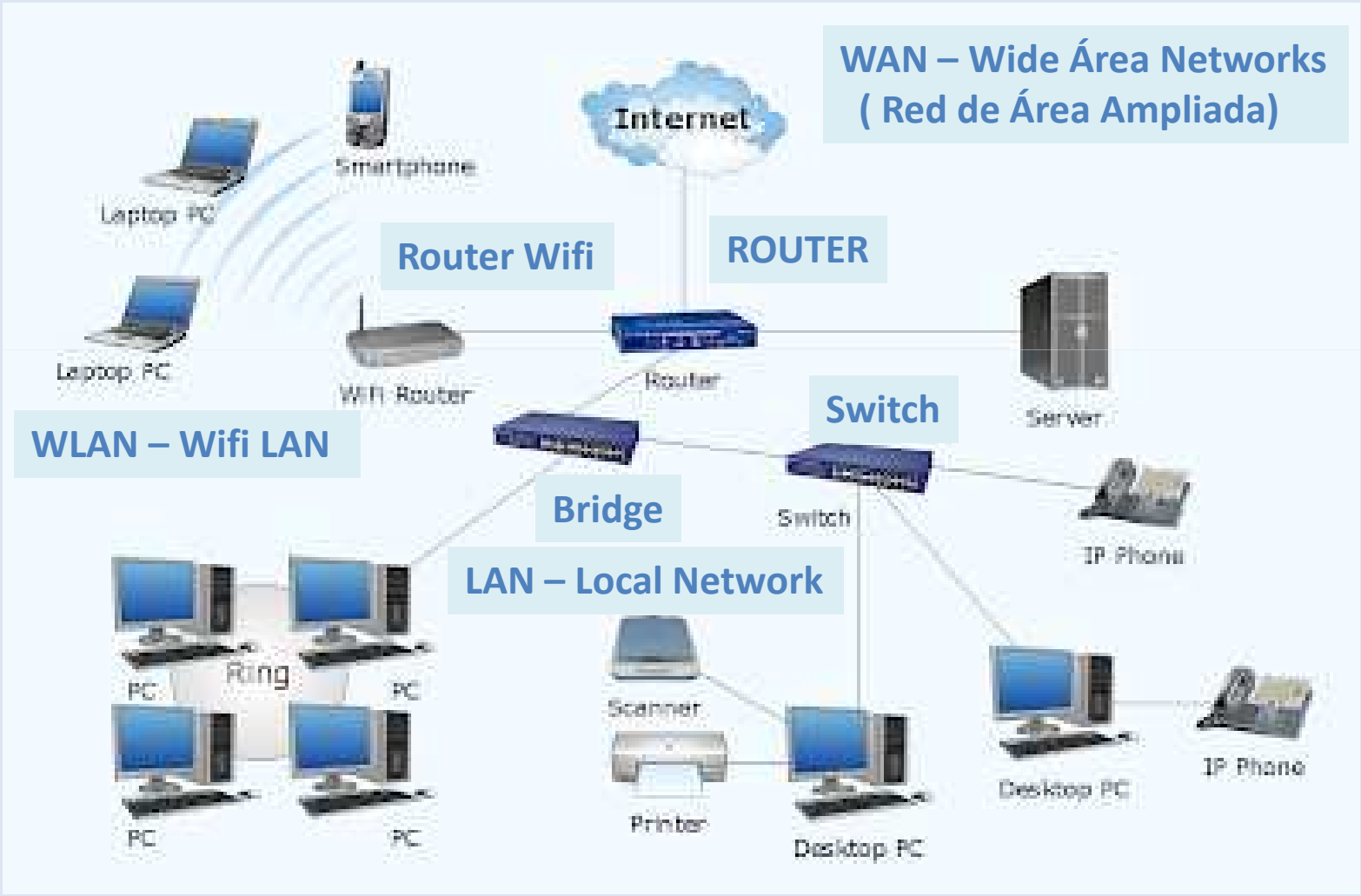
# CONCEPTOS BÁSICOS DE ELEMENTOS DE LA SEGURIDAD DE LA RED

# SET DE HERRAMIENTAS DE LA SEGURIDAD

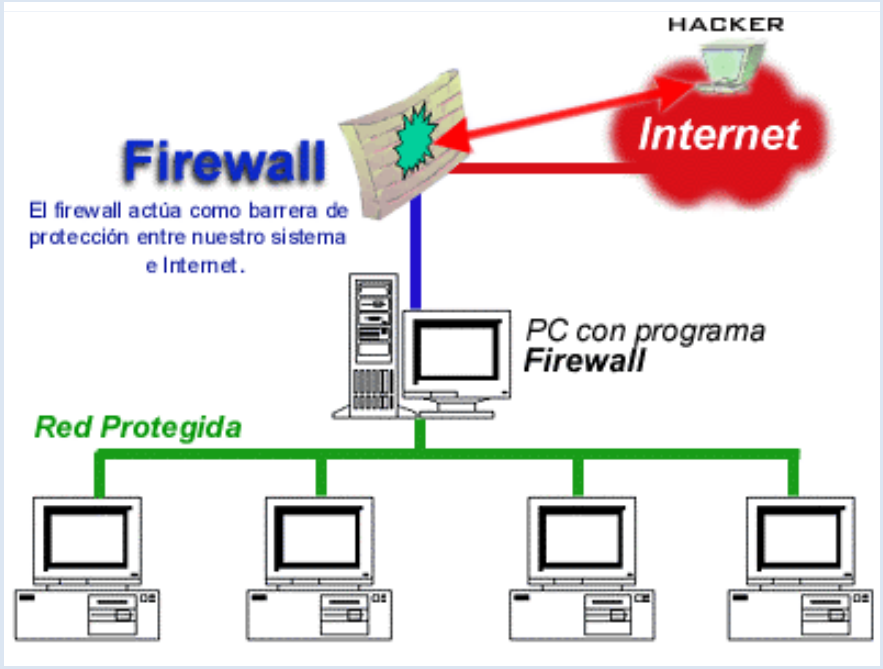

 

# COMPONENTES MÁS COMUNES DE UNA RED



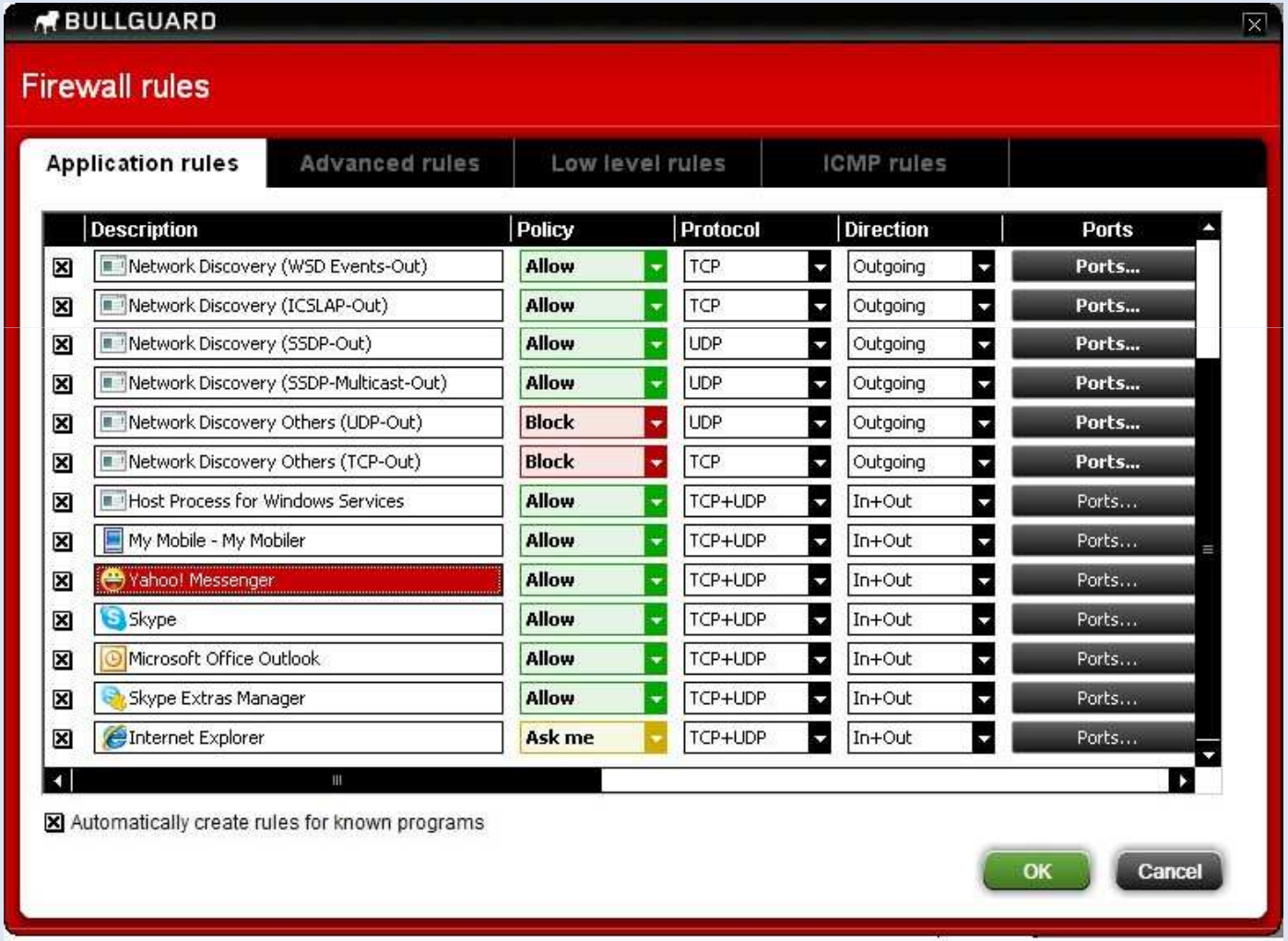
# CORTAFUEGOS – FIREWALL (I)

**Un Cortafuegos o Firewall es un sistema que permite proteger un ordenador o una red de ordenadores de las intrusiones que proviene del exterior del mismo**. Un Firewall puede ser un programa Software o un dispositivo Hardware.

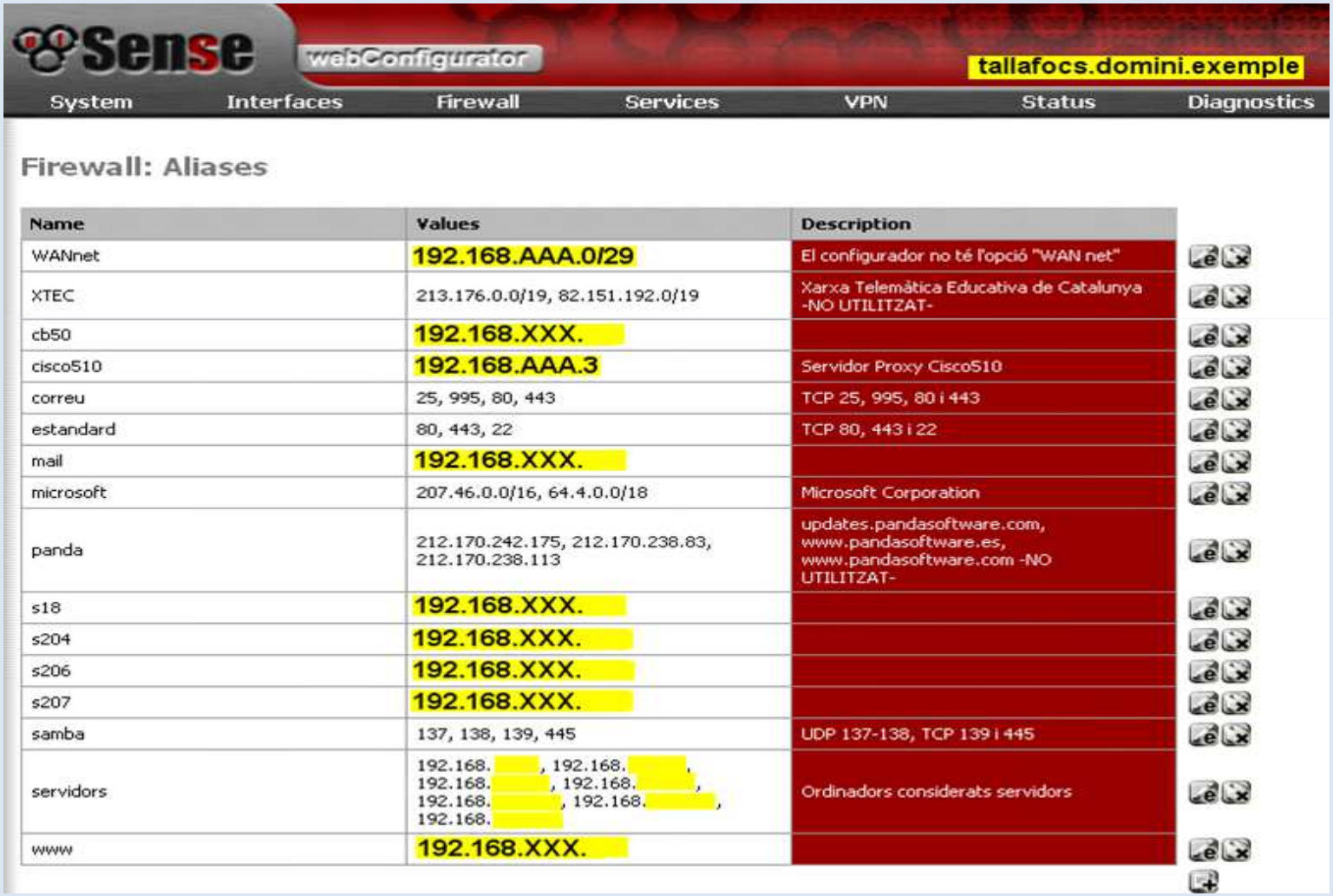



**Un Firewall** se configura con una serie de reglas de tráfico que permite el paso o no de las comunicaciones tanto de entrada como de salida, actuando realmente como un filtro efectivo que puede ser configurado según las necesidades de protección.

# CORTAFUEGOS – FIREWALL / REGLAS POR APLICATIVO



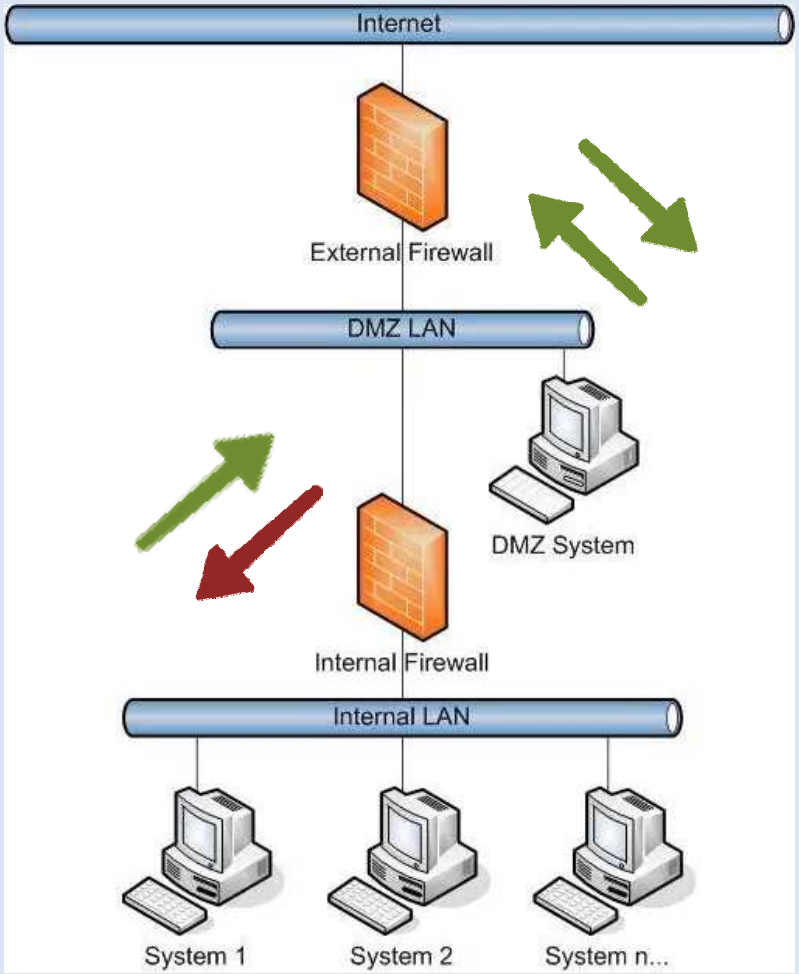
# CORTAFUEGOS – FIREWALL / REGLAS POR PAQUETES




Firewall: Aliases

| Name | Values | Description |
|---|---|---|
| WANnet | 192.168.AAA.0/29 | El configurador no té l'opció "WAN net" |
| XTEC | 213.176.0.0/19, 82.151.192.0/19 | Xarxa Telemàtica Educativa de Catalunya -NO UTILITZAT- |
| cb50 | 192.168.XXX. | |
| cisco510 | 192.168.AAA.3 | Servidor Proxy Cisco510 |
| correu | 25, 995, 80, 443 | TCP 25, 995, 80 i 443 |
| estandard | 80, 443, 22 | TCP 80, 443 i 22 |
| mail | 192.168.XXX. | |
| microsoft | 207.46.0.0/16, 64.4.0.0/18 | Microsoft Corporation |
| panda | 212.170.242.175, 212.170.238.83, 212.170.238.113 | updates.pandasoftware.com, www.pandasoftware.es, www.pandasoftware.com -NO UTILITZAT- |
| s18 | 192.168.XXX. | |
| s204 | 192.168.XXX. | |
| s206 | 192.168.XXX. | |
| s207 | 192.168.XXX. | |
| samba | 137, 138, 139, 445 | UDP 137-138, TCP 139 i 445 |
| servidors | 192.168. , 192.168. , 192.168. , 192.168. , 192.168. , 192.168. , 192.168. | Ordinadors considerats servidors |
| www | 192.168.XXX. | |

## Zona Desmilitarizada – DMZ



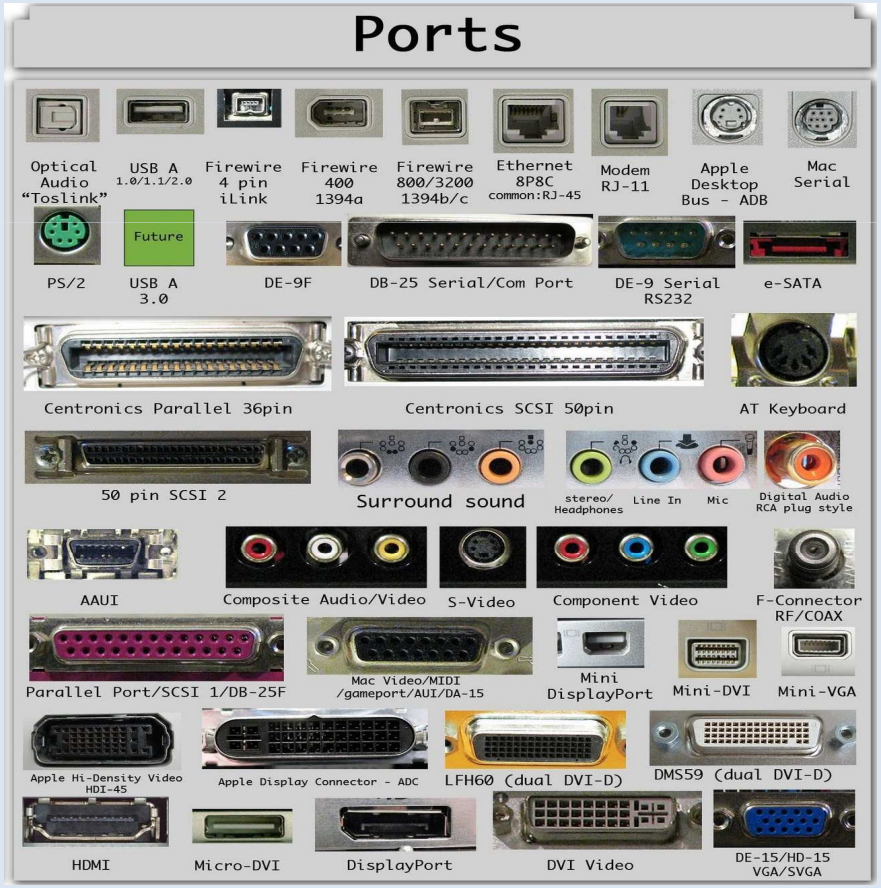

**La DMZ es una zona insegura** que se ubica entre la red interna y la externa (Internet).

**El objetivo de una DMZ** es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que *en general* las conexiones desde la *DMZ* sólo se permitan a la red externa.

**En la DMZ se sitúan los servicios de Correo ; Internet y DNS, WEB de visitas**

# PUERTOS DE COMUNICACIONES

**Un Puerto de Comunicaciones es un interfaz por el cual se permite enviar y recibir información. Los hay físicos y lógicos.**




## PUERTOS DE COMUNICACIONES FÍSICOS

**Son elementos fácilmente identificables en los diferentes dispositivos físicos que conforman la red ( Servidores, PC's, Routes, Bridge, etc.)**

## PUERTOS LÓGICOS DE COMUNICACIONES

►El **Puerto Lógico** es una zona, o localización, de la memoria de un ordenador que se asocia con un puerto físico o con un canal de comunicación, y que proporciona un espacio para el almacenamiento temporal de la información que se va a transferir entre la localización de memoria y el canal de comunicación.

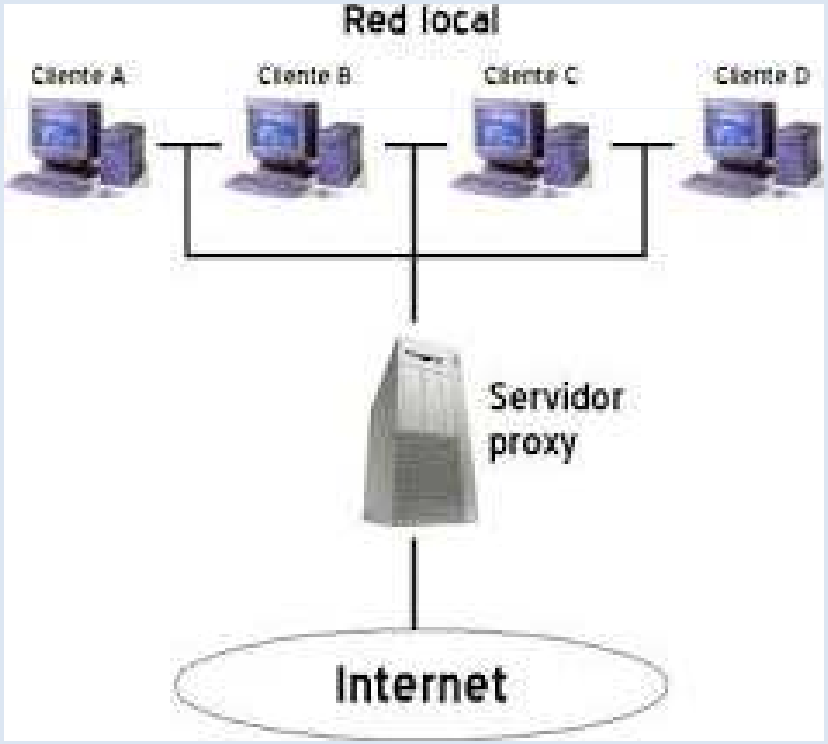
►Un **Puerto Lógico** es el valor que se usa en el modelo de la capa de transporte para distinguir entre las múltiples aplicaciones que se pueden conectar al mismo host, o puesto. Entonces un puerto lógico de Internet es una interface de software que permitirá el ingreso y salida de data por aplicaciones que usan Internet.

►Los **Puertos Lógicos** se identifican por números desde 1 hasta 65.000 pudiendo llegar a mas, siendo conocidos los puertos de 1 a 1024.

## PROXY

Un PROXY es un servidor que actúa a nivel de interfaz de comunicaciones que se sitúa en una posición intermedia ente el navegador de un dispositivo (PC o SmartPhone) y la propia red de Internet.




Cualquier petición que se realice de navegación o visitas de páginas WEB, visualización o descarga pasa por este servidor por lo que sirve de **medio de seguridad, de control y de traza de las conexiones** porque guarda las conexiones y los ficheros a los que se ha accedido, en pocas palabras **es un cuaderno de bitácora de las conexiones y actividades que se realizan entre los dispositivos e Internet.**

# 6 . SEGURIDAD EN LA RED

## Gestión adecuada de la Seguridad (I)

► **Configurar y Parametrizar el acceso a la Red** configurando y creando las reglas necesarias en los FIREWALL, para regular y controlar los accesos externos a la red Interna.

► **Crear e Implementar la división de la RED por medio de la DMZ** situando en la misma aquellos servicios que deban ser accesibles desde el exterior pero que no tengan que estar en la red interna (Servidores de Internet y Dominio, Correo Electrónico, y la Red para visitas).

► **Restringir y Configurar los accesos a los Aplicativos y Puertos** eliminar las **Contraseñas y Puertos por Defecto** de los dispositivos de forma que no sean obvios para los presuntos Ciberdelincuentes complicándoles su labor de intrusión al sistema. **Renovación Periódica de Contraseñas.**

## Gestión adecuada de la Seguridad (II)


► **Limitar la Navegación en Internet** para reducir la exposición a los malware, poner especial atención a los ficheros y/o aplicaciones descargadas e instaladas , conexiones a Redes sociales y a aplicaciones P2P.
Activación de medidas **Antimalware/Antivirus, Antispy, AntiSpam y de Sandbox**.

► **Controlar y gestionar el uso de dispositivos móviles y de almacenamiento externo** (pendrives USB, Discos Externos), activación automática de revisión por Antimalware y Sandbox.

► **Monitorización de las actividades de la red** (tráfico, eventos, niveles utilización y consumo de los recursos disponibles) para identificar sobrecargas y con ello una utilización indebida o bien balancear la carga entre equipos.

# MEDIDAS DE REFUERZO Y MEJORA

# 7 . INFORMACIÓN EN TRÁNSITO

## LA MOVILIDAD

La deslocalización de los puestos de trabajo o la facilitar para la realización de los desempeños laborales de forma deslocalizada (emplazamiento fuera de la empresa, teletrabajo, en las instalaciones del cliente o del proveedor, etc.) hace necesario dotarse de medidas específicas para la seguridad.

### RIESGOS INHERENTES

- **Pérdida/Sustracción** de información confidencial o de dispositivos.
- **Utilización de sistemas de conexión no seguras**, redes propias personales, redes públicas e intercepción de las comunicaciones.
- **Utilización de contextos especiales** como teletrabajo, o BYOD – Bring Your Own Device – "Trae tu propio dispositivo".

## SEGURIDAD EN LOS DISPOSITIVOS DE MOVILIDAD

► Sistemas de encriptado de la información en el disco de los dispositivos físicos ( Encriptadores tipo Bitlocker).

► Posibilidades de bloqueo remoto del dispositivo o borrado de la información del dispositivo.

► Inventario permanente y control de los dispositivos, usuarios, credenciales de acceso, autenticación y permisos asignados.


### MÍNIMOS IMPRESCINDIBLES

► **Incorporación de Antivirus / Antimalware en todos los dispositivos.**

► **Utilización de sistemas de conexión seguras vía VPN y tarjetas o canales propios. Encriptación de las comunicaciones.**

► **Renovación periódica de contraseñas y credenciales.**

► **Control conexiones Bluetooth.**

# 8 . DISPOSITIVOS DE ALMACENAMIENTO

## Gestión Soportes de almacenamiento de la información

► Cualquier proceso de almacenamiento debe cumplir con: **la integridad del sistema, la confidencialidad, preservación, recuperación y disponibilidad de la información**.

► **Debe existir redundancia en la salvaguarda de la información** (copias dobles en tiempo real, sistemas RAID, copias en caliente, etc.).

► **Redundancia con deslocalización de las copias de seguridad.** Dispositivos externos deslocalizados o copia en la nube para copias de respaldo de la información.

►**Dispositivos de Almacenamiento local o servidores en la red para el trabajo directo.**

► **Controles periódicos de recuperación y restauración.**

# 9 . REGISTRO DE LA ACTIVIDAD

# REGISTRO DE LA ACTIVIDAD

El registro de la actividad **permite detectar posible problemas o deficiencias en los sistemas y aplicativos** recopilando información relativa al estado y disponibilidad de los dispositivos, niveles de almacenaje, el tráfico de la red, picos o saturaciones de actividad, errores y avisos, etc.


## TIPOS DE MONITORIZADO

► **DE LOS SISTEMAS Y APLICATIVOS DURANTE LA EXPLOTACIÓN** se realizan por medio de herramientas que **monitorizan el normal funcionamiento del día a día del sistema y los aplicativos** .

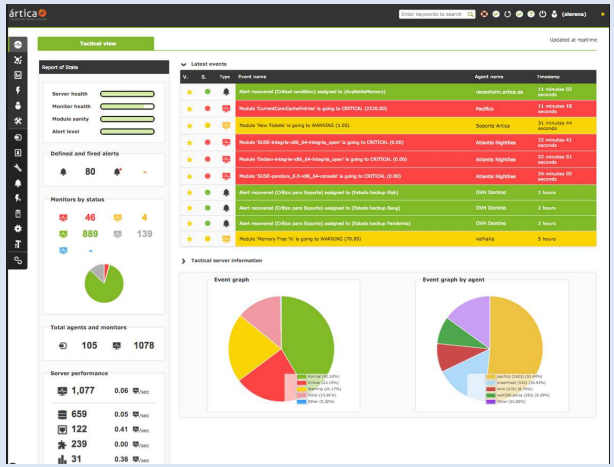
► **DE SEGURIDAD** es una **monitorización y seguimiento específico dirigido a detectar fallos de seguridad e intrusos.**

► **DE ACTIVIDAD DE USUARIOS** seguimiento específico a usuarios.

# MONITORIZACIÓN DE SISTEMAS Y APLICATIVOS

El objetivo final del seguimiento y monitorización de los sistemas y la infraestructura es la de garantizar la disponibilidad y el rendimiento de los mismos, detectando errores, deficiencias y sobrecargas para tomar las decisiones correctivas.



## Monitorización de Sistemas y Aplicativos

► **Un incremento de la visibilidad y entendimiento de la red e infraestructura.**

► **Una mejora** en la exactitud y precisión **en la detección de anomalías y alertas** facilitando el diagnóstico y la resolución de problemas.

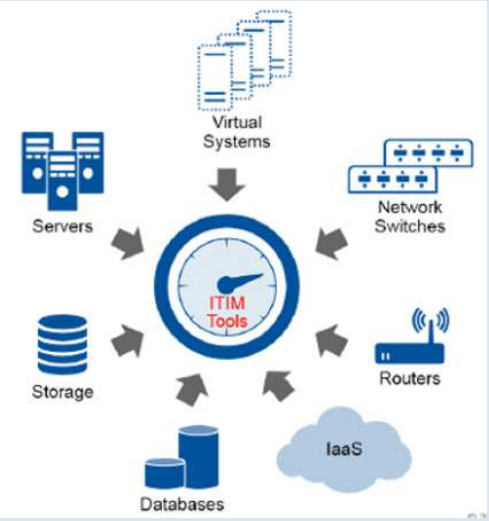
► **Una reducción en las interrupciones y un incremento de la disponibilidad de los dispositivos y aplicativos.**

► Una integración con el análisis y correlación de eventos con **visibilidad centralizada y un mejor análisis.**

# MONITORIZACIÓN DE SEGURIDAD

El objetivo final de la monitorización de Seguridad es la recolección de información y datos relativos a los elementos de seguridad, detección de las posibles anomalías y el análisis de la información para identificar, mitigar o corregir fallos de Seguridad.

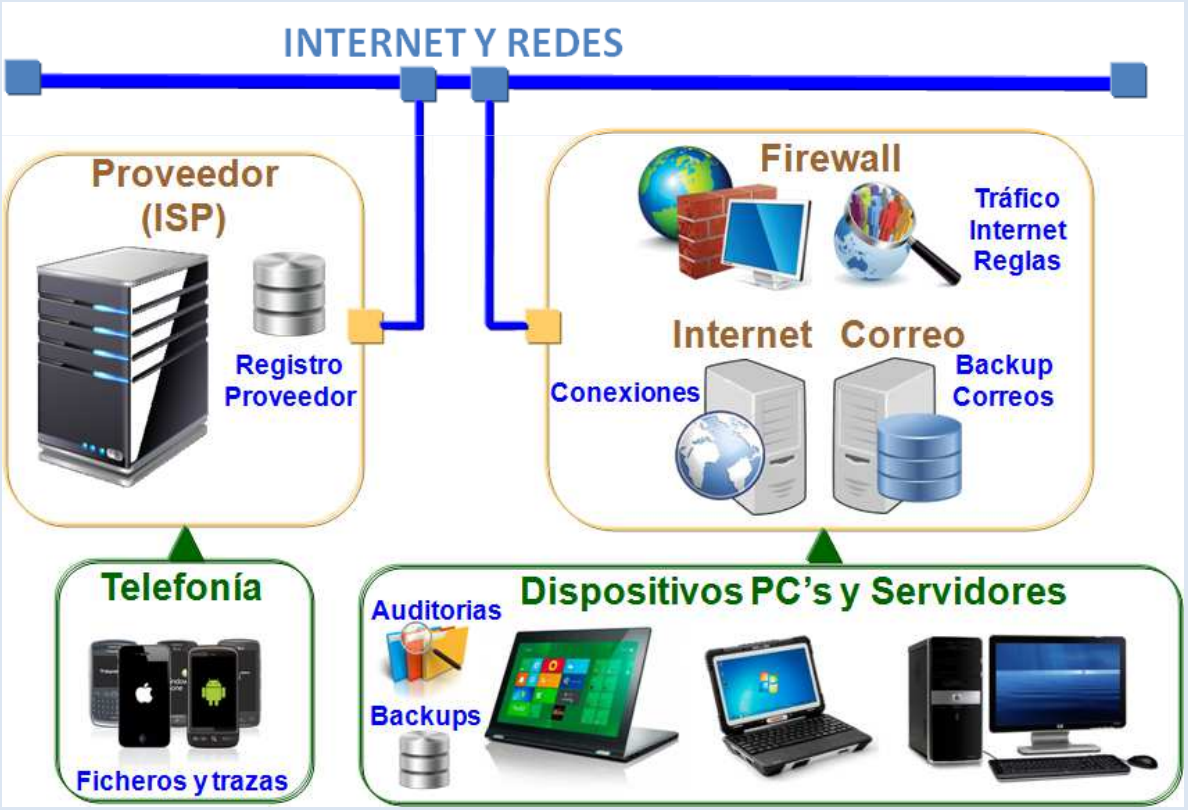



## Tipología de Eventos de Seguridad a Monitorizar

- **Trafico en la red** entre dispositivos y aplicativos.
- **Accesos a los sistemas o aplicativos :** autorizados, rechazados, fuera de horario, no habituales.
- **Cambios de configuración y usos de autorizaciones especiales.**
- **Avisos de los Antimalware/Antivirus.**
- **Alarmas y avisos de incidentes** generados por los dispositivos o aplicativos.

# MONITORIZACIÓN DE LAS ACTIVIDADES DE UN USUARIO

En ocasiones puede ser necesario el seguimiento de la actividad y utilización de los medios de la empresa que realiza un usuario en concreto, en especial, en investigaciones o seguimiento cuando se sospecha que esta llevando a cabo una actividad ilícita o bien que rompe la buena fe empresarial.



# SISTEMAS DE IDENTIFICACIÓN DE INTRUSOS - IDS

El objetivo del IDS es la identificación de intrusos (software o atacante) por medio del análisis de la red o del comportamiento de los dispositivos.

**IDS basados en la Red**

► **Basados en la Firma,** examina los paquetes de información el trafico de la red en búsqueda de firmas y patrones conocidos para alertar de su presencia, funciona de forma parecida a los Antivirus.

► **Basados en Anomalías,** examina la actividad inusual que se identifica que se desvía de los promedios o es no contemplada.

**IDS basados en el Cliente**

► **Basados en la Actividad Interna** desarrollada por el dispositivo analizando los log's o trazas del sistema , las versiones de los programas y archivos claves, etc.

# 10 . CONTINUIDAD DEL NEGOCIO

# CONTINUIDAD DEL NEGOCIO

Ante incidentes de Seguridad es necesario proteger los principales procesos de negocio a través de un conjunto de medidas que permitan a la Organización recuperarse en el menor espacio posible de tiempo de un incidente posibilitando la continuación del negocio evitando el bloqueo o pérdidas en el mismo.


## Objetivos de la Continuidad del Negocio

► **Evitar que las actividades de la empresa se interrumpan o** si lo hacen sea **el menor tiempo posible.**

► **Establecer un proceso de recuperación,** con actores y responsables y tiempo de respuesta y recuperación máximo

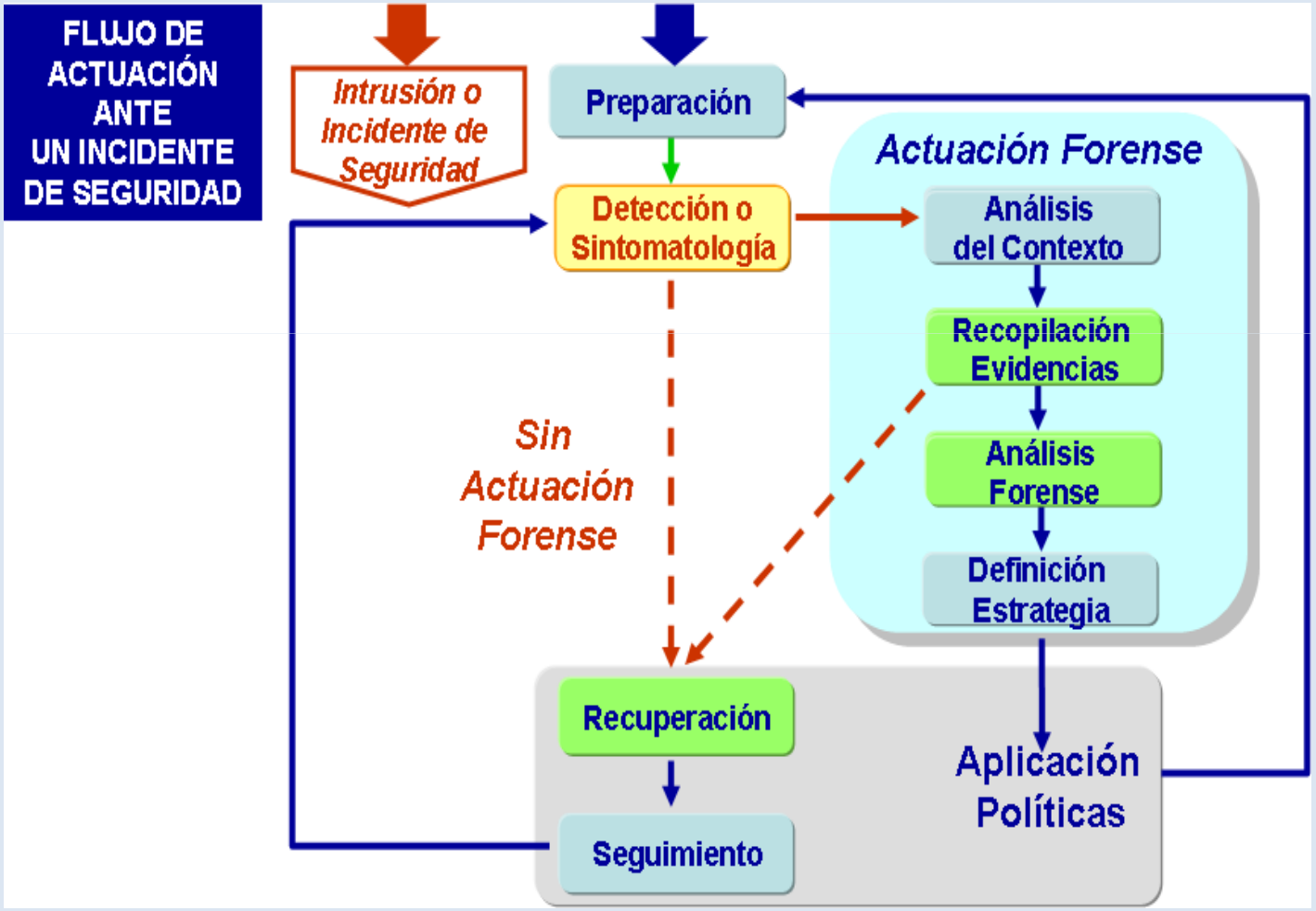
► **Ser capaces de restituir la situación inicial previa.**

► **Analizar los incidentes,** causas, impacto y **diseñar medidas** preventivas, alarmas y avisos, medidas correctivas, de mejora a aplicar a la situación actual.

## PLAN BÁSICO DE CONTINUIDAD DEL NEGOCIO
## PLANIFICACIÓN DE RECUPERACIÓN DE DESASTRES (DRP)

## ESQUEMA DE ACTUACIÓN ANTE UN INCIDENTE DE SEGURIDAD



# SOPORTE DE UN CERT/CSIRT

**CERT:** Computer Emergency Response Team (equipo de respuesta a emergencias informáticas)

**CSIRT:** Computer Security Incident Response Team (equipo de respuesta a incidentes de seguridad informática)

| Características/Sitios | INCIBE | UNAM-CERT | INFOTEC | CERT | US-CERT | CERT-EU | NCI | ENISA | TERENA | TF-CSIRT |
|---|---|---|---|---|---|---|---|---|---|---|
| Acerca de | Si | Si | Si | Si | Si | Si | Si | Si | Si | Si |
| FAQ | Si | No | Si | Si | Si | No | No | No | No | No |
| Misión y objetivos | Si | Si | Si | Si | Si | No | Si | Si | No | No |
| Contacto | No | Si | Si | Si | Si | Si | Si | Si | Si | Si |
| Eventos | Si | Si | Si | Si | Si | Si | Si | Si | Si | Si |
| Documentos | Si | Si | Si | Si | Si | Si | No | Si | Si | No |
| Herramientas | Si | Si | Si | No | No | Si | No | Si | No | No |
| Vulnerabilidades | Si | Si | No | Si | Si | Si | No | No | No | No |
| Noticias | Si | Si | Si | Si | Si | Si | Si | Si | Si | Si |
| Indicadores/estadísticas | No | Si | No | No | No | Si | No | No | No | No |
| Enlaces (sitios relacionados) | Si | Si | Si | Si | Si | Si | Si | Si | Si | Si |
| Seguridad en tu idioma/Tips | No | Si | No | No | Si | No | No | No | No | No |
| Blogs | Si | No | No | Si | No | No | No | No | No | No |
| Cursos | No | No | No | Si | No | No | No | Si | No | Si |
| Reporte de Incidencias | Si | Si | No | Si* | Si* | No | No | No | No | No |
| Suscripción a alertas | Si | Si | No | Si | Si | Si | Si | Si | Si | No |
| Redes Sociales | Si | Si | Si | Si | Si | No | No | Si | Si | No |

Tabla 2 – Cuadro de análisis comparativo entre 10 sitios CSIRT/CERT

# PREGUNTAS

**Rafael López Rivera**

**Perito Informático y Tecnológico**

***Vicepresidente de la ACPJT***
***Fundador de: APTAN y ANCITE***
***Miembro de: Stop Violencia de Género Digital y Aspertic***

| | |
|---|---|
| **Graduado en DERECHO** | **- Derecho.** |
| **Licenciado en ADE** | **- Administración y Dirección de Empresas.** |
| **Licenciado en CT** | **- Ciencias del Trabajo – Laboral (Graduado Social).** |
| **Licenciado en ITM** | **- Investigación y Técnicas de Mercado (Estadística).** |
| **Diplomado en CCEE** | **- Ciencias Empresariales.** |
| **Ingeniero Técnico Industrial** | **- Ingeniería.** |

**Masters Universitarios: PDD, GDE, DAI , DPD, Compliance Officer.**
**Certificaciones Internacionales: PMP, PRINCE2, ITIL 2 / 3, SAP, OEM101**
**Técnico Superior en Seguridad Informática por la UCAV-SEAS**

***www.peritoit.com***
***peritoit@hotmail.com***
http://es.linkedin.com/in/rafaellopezrivera
***606 944 394***