# Apuntes de Seguridad y alta disponibilidad Documentation

*Versión 1.0*

**Oscar GG**

**23 de septiembre de 2019**

# Contenidos:


**1. Adopción de pautas de seguridad informática** **1**
- 1.1. Fiabilidad, confidencialidad, integridad y disponibilidad. . . . 1
- 1.2. Elementos vulnerables en el sistema informático; hardware, software y datos. . . . 1
- 1.3. Análisis de las principales vulnerabilidades de un sistema informático. . . . 2
- 1.4. Amenazas. Tipos. . . . 2
- 1.5. Amenazas físicas. . . . 5
- 1.6. Amenazas lógicas. . . . 5
- 1.7. Seguridad física y ambiental . . . 5
- 1.8. Ubicación y protección física de los equipos y servidores. . . . 5
- 1.9. Sistemas de alimentación ininterrumpida. . . . 5
- 1.10. Seguridad lógica. . . . 5
- 1.11. Criptografía. . . . 5
- 1.12. Listas de control de acceso. . . . 5
- 1.13. Establecimiento de políticas de contraseñas. . . . 5
- 1.14. Políticas de almacenamiento. . . . 5
- 1.15. Copias de seguridad e imágenes de respaldo. . . . 5
- 1.16. Medios de almacenamiento. . . . 5
- 1.17. Sistemas biométricos. Funcionamiento. Estándares. . . . 5
- 1.18. Análisis forense en sistemas informáticos . . . 5
- 1.19. Funcionalidad y fases de un análisis forense. . . . 5
- 1.20. Respuesta a incidentes. . . . 5
- 1.21. Análisis de evidencias digitales. . . . 5
- 1.22. Herramientas de análisis forense. . . . 5
- 1.23. El sistema operativo Unix . . . 5

**2. Legislación y normas sobre seguridad** **7**
- 2.1. Legislación sobre protección de datos. . . . 7
- 2.2. La Ley Orgánica de Protección de Datos . . . 7
  - 2.2.1. Artículo 1. Objeto de la Ley . . . 7
  - 2.2.2. Artículo 2. Ámbito de aplicación . . . 7
  - 2.2.3. Artículo 3. Datos de fallecidos . . . 7
  - 2.2.4. Artículo 4. Exactitud de los datos . . . 7
  - 2.2.5. Artículo 5. Deber de confidencialidad. . . . 8
  - 2.2.6. Artículo 6. Tratamiento basado en el consentimiento del afectado. . . . 8
  - 2.2.7. Artículo 7. Consentimiento de los menores de edad. . . . 8

2.2.8. Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos. . . . 8
2.2.9. Artículo 9. Categorías especiales de datos. . . . 8
2.2.10. Artículo 10. Tratamiento de datos de naturaleza penal. . . . 8
2.2.11. Artículo 11. Transparencia e información al afectado. . . . 8
2.2.12. Artículo 12. Disposiciones generales sobre ejercicio de los derechos. . . . 8

**3. Implantación de técnicas de acceso remoto. Seguridad perimetral 9**
3.1. Elementos básicos de la seguridad perimetral. . . . 10
3.2. Perímetros de red. Zonas desmilitarizadas. Router frontera. . . . 10
3.3. Arquitectura débil de subred protegida. . . . 10
3.4. Arquitectura fuerte de subred protegida. . . . 10
3.5. Políticas de defensa en profundidad. . . . 10
3.6. Defensa perimetral. . . . 10
3.7. Defensa interna. . . . 10
3.8. Factor Humano. . . . 10
3.9. Redes privadas virtuales. VPN. . . . 10
3.10. Beneficios y desventajas con respecto a las líneas dedicadas. . . . 10
3.11. Técnicas de cifrado. Clave pública y clave privada. . . . 10
3.12. VPN a nivel de enlace. . . . 10
3.13. VPN a nivel de red. SSL, Pisac. . . . 10
3.14. VPN a nivel de aplicación. SSH. . . . 10
3.15. Intérprete de comandos SSH. . . . 10
3.16. Gestión de archivos SSH. . . . 10
3.17. Servidores de acceso remoto . . . 10
3.18. Protocolos de autenticación. . . . 10
3.19. Configuración de parámetros de acceso. . . . 10
3.20. Servidores de autenticación. . . . 10

**4. Instalación y configuración de cortafuegos 11**
4.1. Utilización de cortafuegos. . . . 11
4.2. Filtrado de paquetes de datos. . . . 11
4.3. Tipos de cortafuegos. Características. Funciones principal. . . . 11
4.4. Instalación de cortafuegos. Ubicación. . . . 11
4.5. Reglas de filtrado de cortafuegos. . . . 11
4.6. Pruebas de funcionamiento. Sondeo. . . . 11
4.7. Registros de sucesos de un cortafuegos. . . . 11
4.8. Cortafuegos integrados en los sistemas operativos. . . . 11
4.9. Cortafuegos libres y propietarios. . . . 11
4.10. Distribuciones libres para implementar cortafuegos en máquinas dedicadas. . . . 11
4.11. Cortafuegos hardware. . . . 11

**5. Instalación y configuración de servidores proxy 13**
5.1. Tipos de proxy . Características y funciones. . . . 13
5.2. Instalación de servidores proxy . . . 13
5.3. Instalación y configuración de clientes proxy . . . 13
5.4. Configuración del almacenamiento en la caché de un proxy . . . 13
5.5. Configuración de filtros. . . . 13
5.6. Métodos de autenticación en un proxy . . . 13
5.7. Proxys inversos. . . . 13
5.8. Proxys encadenados. . . . 13
5.9. Pruebas de funcionamiento. Herramientas gráficas. . . . 13

**6. Implantación de soluciones de alta disponibilidad 15**
6.1. Definición y objetivos. . . . 16

6.2. Análisis de configuraciones de alta disponibilidad . . . 16
6.3. Funcionamiento ininterrumpido. . . . 16
6.4. Integridad de datos y recuperación de servicio. . . . 16
6.5. Servidores redundantes. . . . 16
6.6. Sistemas de clusters . . . 16
6.7. SAN, NAS, FiberChannel . . . 16
6.8. Balanceadores de carga. . . . 16
6.9. Instalación y configuración de soluciones de alta disponibilidad. . . . 16
6.10. Vitalización de sistemas. . . . 16
6.11. Posibilidades de la virtualización de sistemas. . . . 16
6.12. Herramientas para la virtualización. . . . 16
6.13. Configuración y utilización de maquinas virtuales. . . . 16
6.14. Alta disponibilidad y virtualización. . . . 16
6.15. Simulación de servicios con virtualización. . . . 16

# CAPÍTULO 1

# Adopción de pautas de seguridad informática

## 1.1 Fiabilidad, confidencialidad, integridad y disponibilidad.

A continuación definimos los siguientes términos

- Fiabilidad: la capacidad de conseguir que un SI ofrezca la información sin pausas entre peticiones.
- confidencialidad: capacidad de conseguir que la información se muestre solo a las personas que estén autorizadas para ello.
- Integridad: capacidad de conseguir que la información no se altere por causas involuntarias.
- Disponibilidad: capacidad de respuesta a una peticiones con las mínimas pausas por causas involuntarias.

En relación con el último punto, se mide la disponibilidad de un SI en «nueves».

- Se dice que un SI ofrece una disponibilidad de «2 nueves», si está disponible el 99 % del tiempo.
- Se dice que un SI ofrece una disponibilidad de «3 nueves», si lo está al 99.9 %.
- Se dice que un SI ofrece una disponibilidad de «4 nueves» si lo está al 99.99 %.
- Se dice que un SI ofrece una disponibilidad de «5 nueves» si lo está al 99.999 %

Ejercicio: Si un año tiene 365 días, calcular cuanto tiempo podría estar como «no disponible» cada uno de los sistemas que hemos enumerado en el punto anterior.

## 1.2 Elementos vulnerables en el sistema informático; hardware, software y datos.

«Vulnerable»: medida de la capacidad de un sistema para fallar de manera inesperada. En pocas palabras una vulnerabilidad es un punto débil.

Como resulta evidente en un SI hay tres grandes elementos que son susceptibles de ser vulnerables:

- **Hardware.**

    - Fluido eléctrico.
    - Placa base.
    - RAM: errores muy difíciles de detectar.
    - Discos: hay abundantes estadísticas acerca de sus tasas de fallos.
    - Tarjetas gráficas.
    - Interconexiones. cables y/o soldaduras
- **Software.**
    - Sistema operativo: es importante tener activada la actualización automática que aplica «parches» sin necesidad de recordar aplicarlas manualmente. Para evitar la aplicación de actualizaciones que puedan estropear otras partes se suele aconsejar NO TENER ACTIVADA LA ACTUALIZACIÓN AUTOMÁTICA en equipos críticos y sí tenerla en otros equipos que actúen como «cobayas.»
    - Aplicaciones. También pueden mostrar fallos que den lugar a consecuencias muy desagradables especialmente con los datos.
- Datos. Hoy en día son casi con total seguridad el activo más valioso de la empresa. Para protegerlos habrá que tomar muchas medidas de seguridad.

## 1.3 Análisis de las principales vulnerabilidades de un sistema informático.

Cuando se habla de vulnerabilidad, se asocia este término con problemas software. Una vulnerabilidad puede conllevar una serie de problemas muy graves:

- Que un intruso consiga permisos de administración en un sistema.
- Que un virus informático consiga tomar el control de los equipos de la empresa.
- Que un software o individuo consiga borrar/alterar/cifrar datos de la empresa.

En Internet todas las vulnerabilidades detectadas se publican como un informe CVE (Common Vulnerability Exposure)

Recientemente se han descubierto **vulnerabilidades a nivel de microprocesador**. En entornos muy sofisticados existen unas vulnerabilidades llamadas TEMPEST.

Algunas aplicaciones basadas en bases de datos son susceptibles de sufrir «ataques SQL» o «inyecciones SQL» o «SQL injects».

Otro tipo de ataque común son los HTML/JS injects.

En líneas generales, ningún programa web debe confiar en lo que escriben sus usuarios.

## 1.4 Amenazas. Tipos.

Clasificando por lugar

- Interna
- Externa

Clasificando por mecanismo

- Físicas

- Lógicas

## 1.5 Amenazas físicas.

## 1.6 Amenazas lógicas.

## 1.7 Seguridad física y ambiental

## 1.8 Ubicación y protección física de los equipos y servidores.

## 1.9 Sistemas de alimentación ininterrumpida.

## 1.10 Seguridad lógica.

## 1.11 Criptografía.

## 1.12 Listas de control de acceso.

## 1.13 Establecimiento de políticas de contraseñas.

## 1.14 Políticas de almacenamiento.

## 1.15 Copias de seguridad e imágenes de respaldo.

## 1.16 Medios de almacenamiento.

## 1.17 Sistemas biométricos. Funcionamiento. Estándares.

## 1.18 Análisis forense en sistemas informáticos

## 1.19 Funcionalidad y fases de un análisis forense.

## 1.20 Respuesta a incidentes.

## 1.21 Análisis de evidencias digitales.

## 1.22 Herramientas de análisis forense.

## 1.23 El sistema operativo Unix

A lo largo del curso usaremos GNU/Linux, un sistema operativo de tipo UNIX de libre distribución. Aunque GNU/Linux suele empaquetarse en «distribuciones» que suelen incluir un entorno gráfico en este módulo aprende-

remos a movernos por el sistema utilizando los comandos.

- `mkdir` nos permite crear directorios.
- `cd` nos permite movernos a un directorio.
- `rm` nos permite borrar ficheros.
- `rmdir` nos permite borrar un directorio **siempre y cuando esté vacío**.
- `ls` muestra los ficheros del directorio actual.
- `cat` nos permite imprimir un fichero por pantalla.
- `man <comando>` nos permite obtener ayuda sobre un cierto comando (o incluso fichero de configuración).
- `pwd` nos muestra el nombre del directorio actual.
- `nano` nos da acceso a un pequeño editor de texto que nos permitirá editar, entre otras cosas, los ficheros de configuración del sistema.
- Cuando se manipulan ficheros se puede ocultar un fichero *usando el punto como primer carácter de un fichero*.
- `apt-get` nos permitirá instalar sofware de los repositorios del empaquetador de la distribución.
- Se puede ejecutar un comando escribiendo el nombre de dicho comando. Si el comando no está en las rutas de búsqueda se puede escribir la ruta completa.
- Se puede redirigir la salida de un comando hacia un fichero (usando `<comando> > <fichero>` o redirigir la salida de un comando hacia otro comando con `<comando> | <comando>`
- Un comando de cualquier tipo podría necesitar **permisos de administrador**. En ese caso tendremos que usar el comando `sudo` de esta manera: `sudo <comando>` .

CAPÍTULO 2

# Legislación y normas sobre seguridad

## 2.1 Legislación sobre protección de datos.

## 2.2 La Ley Orgánica de Protección de Datos

### 2.2.1 Artículo 1. Objeto de la Ley

### 2.2.2 Artículo 2. Ámbito de aplicación

Ficheros automatizados pero sin incluir información clasificada y que estén dentro del ámbito de la UE (si están fuera de la UE se estará a los dispuesta en «su legislación específica»). Los datos resultado de procesos judiciales se incluyen en este fichero sin incluir otras disposiciones que se puedan aplicar debido a la Ley del Poder Judicial.

### 2.2.3 Artículo 3. Datos de fallecidos

- Los familiares de un fallecido pueden acceder a sus datos. Hay una excepción: el fallecido podría haber prohibido dicho acceso.
- El fallecido puede permitir acceso a otros, aparte de sus familiares.

### 2.2.4 Artículo 4. Exactitud de los datos

Los datos deberán ser exactos y actualizados. Si no es así se puede imputar al responsable excepto que:

- Los datos vengan del propio afectado (es decir, mintió)
- Los datos provengan de un mediador (se imputará al mediador).
- Los datos fueran procesados por otro responsable.
- Los datos se obtuvieran de un registro público.

### 2.2.5 Artículo 5. Deber de confidencialidad.

Se debe guardar el secreto profesional **incluso despues de dejar de ser el responsable**

### 2.2.6 Artículo 6. Tratamiento basado en el consentimiento del afectado.

El afectado debe dar su consentimiento claramente. Si se pide el consentimiento para muchas finalidades, se debe indicar claramente que se pide para todas. **No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.**

### 2.2.7 Artículo 7. Consentimiento de los menores de edad.

Solo se acepta el consentimiento de los mayores de 14. Solo se acepta el consentimiento de los menores de 14 si el consentimiento de sus tutores también aparece.

### 2.2.8 Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.

El reglamento de la UE es el que dice cuando un tratamiento de datos es una obligación legal o un interés público. P.ej, impuestos o censos.

### 2.2.9 Artículo 9. Categorías especiales de datos.

En general: ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico. Hay algunas excepciones, como por ejemplo una fundación, ONG o sindicato.

### 2.2.10 Artículo 10. Tratamiento de datos de naturaleza penal.

Los datos penales no podrán usarse para otros fines y su tratamiento solo podrá hacerse por abogados y procuradores.

### 2.2.11 Artículo 11. Transparencia e información al afectado.

El responsable debe cumplir con el deber de información y decir al afectado:

1. La identidad del responsable o su representante.
2. La finalidad del tratamiento.
3. La posibilidad de ejercer sus derechos a modificación, borrado o cancelación.

### 2.2.12 Artículo 12. Disposiciones generales sobre ejercicio de los derechos.

- El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden.
- La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable
- Las actividades del responsable serán gratuitas.

# CAPÍTULO 3

## Implantación de técnicas de acceso remoto. Seguridad perimetral


### 3.1 Elementos básicos de la seguridad perimetral.

### 3.2 Perímetros de red. Zonas desmilitarizadas. Router frontera.

### 3.3 Arquitectura débil de subred protegida.

### 3.4 Arquitectura fuerte de subred protegida.

### 3.5 Políticas de defensa en profundidad.

### 3.6 Defensa perimetral.

### 3.7 Defensa interna.

### 3.8 Factor Humano.

### 3.9 Redes privadas virtuales. VPN.

### 3.10 Beneficios y desventajas con respecto a las líneas dedicadas.

### 3.11 Técnicas de cifrado. Clave pública y clave privada.

### 3.12 VPN a nivel de enlace.

### 3.13 VPN a nivel de red. SSL, Pfsac.

### 3.14 VPN a nivel de aplicación. SSH.

CAPÍTULO 4

# Instalación y configuración de cortafuegos

**4.1 Utilización de cortafuegos.**

**4.2 Filtrado de paquetes de datos.**

**4.3 Tipos de cortafuegos. Características. Funciones principal.**

**4.4 Instalación de cortafuegos. Ubicación.**

**4.5 Reglas de filtrado de cortafuegos.**

**4.6 Pruebas de funcionamiento. Sondeo.**

**4.7 Registros de sucesos de un cortafuegos.**

**4.8 Cortafuegos integrados en los sistemas operativos.**

**4.9 Cortafuegos libres y propietarios.**

**4.10 Distribuciones libres para implementar cortafuegos en máquinas dedicadas.**

**4.11 Cortafuegos hardware.**

CAPÍTULO 5

# Instalación y configuración de servidores proxy

## 5.1 Tipos de proxy . Características y funciones.

## 5.2 Instalación de servidores proxy .

## 5.3 Instalación y configuración de clientes proxy .

## 5.4 Configuración del almacenamiento en la caché de un proxy .

## 5.5 Configuración de filtros.

## 5.6 Métodos de autenticación en un proxy .

## 5.7 Proxys inversos.

## 5.8 Proxys encadenados.

## 5.9 Pruebas de funcionamiento. Herramientas gráficas.

CAPÍTULO 6

# Implantación de soluciones de alta disponibilidad


## 6.1 Definición y objetivos.

## 6.2 Análisis de configuraciones de alta disponibilidad

## 6.3 Funcionamiento ininterrumpido.

## 6.4 Integridad de datos y recuperación de servicio.

## 6.5 Servidores redundantes.

## 6.6 Sistemas de clusters .

## 6.7 SAN, NAS, FiberChannel

## 6.8 Balanceadores de carga.

## 6.9 Instalación y configuración de soluciones de alta disponibilidad.

## 6.10 Vitalización de sistemas.

## 6.11 Posibilidades de la virtualización de sistemas.

## 6.12 Herramientas para la virtualización.

## 6.13 Configuración y utilización de máquinas virtuales.

## 6.14 Alta disponibilidad y virtualización.