UNIVERSIDAD DE GRANADA

[TALLER T3]

HERRAMIENTAS CONTRA EL CIBERDELITO:

SEGURIDAD Y PRIVACIDAD CON FUENTES ABIERTAS

José Antonio Gómez Hernández, 2018

Oficina de Software Libre

Jornadas de Software Libre de la UGR

Granada, 27-28 de septiembre de 2018

TABLA DE CONTENIDOS

01

JOSÉ ANTONIO GÓMEZ HERNÁNDEZ

- Grupo de investigación: ***Network Engineering and Security Group*** - **NESG**, https://nesg.ugr.es.
- Profesor del Departamento de ***Lenguajes y Sistemas Informáticos***.
- Imparto docencia en Ciberseguridad en el Grado de Ingeniería Informática, el Grado de Criminología, y el Máster Propio en Ciberseguridad.
- Mi correo: **jagomez@ugr.es**.

02

OBJETIVO DEL TALLER

- Conocer herramientas básicas de fuentes abiertas para mantener nuestros sistemas seguros frente a diferentes tipos de ataques y mantener un mínimo de privacidad.

03

JUSTIFICACIÓN DEL TALLER

- Los ciberdelincuentes tratan de acceder a nuestros sistemas como medio para obtener nuestra información, para acceder a otros sistemas, utilizar nuestros recursos, etc.
- Somos un eslabón, quizás el más débil, en la seguridad de la red.
- Prevenir/detectar ataques a nuestros sistemas y/o evitar el acceso a nuestros datos privados, puede evitarnos problemas.

04

CIBERSEGURIDAD

1 COPIAS DE SEGURIDAD

Copias de seguridad con ***Déjà dup***.

2 ANTIVIRUS

Detectar malware con ***ClamAV***.

3 GESTOR DE CONTRASEÑAS

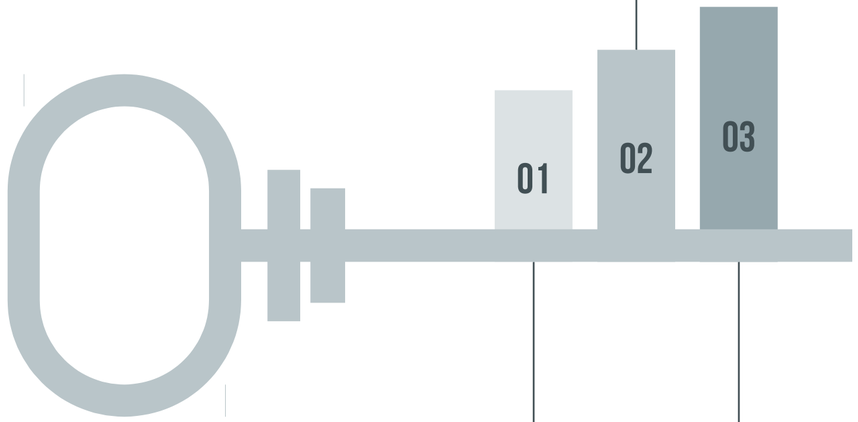
Asegurar todas nuestras contraseñas con ***KeePass***.

4 ACTUALIZACIONES DE SOFTWARE

.

1 COPIAS DE SEGURIDAD

DEJA DUP



PASO 1: INSTALAR/EJECUTAR

- En versiones recientes ya esta instalado
- Si no, instalar software *dejadup*:

```
sudo apt-get installdeja-dup
```

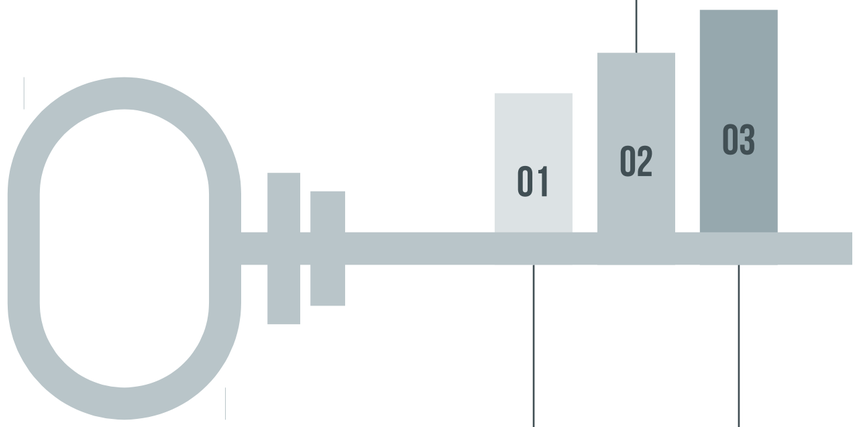
PASO 2: CONFIGURAR

1 – Seleccionar la carpeta a copiar (nuestro directorio de trabajo).
2 – Seleccionar el destino (disco duro, ..)
3 – Establecer planificación automática.

PASO 3: ACTIVAR

- Activar la copia de seguridad.

2 ANTIMALWARE
CLAMAV



PASO 2: CONFIGURAR

1 – Actualizar patrones de malware.

2 – Configurar.

[3 – Lista Blanca.]

[4 – Planificar.]

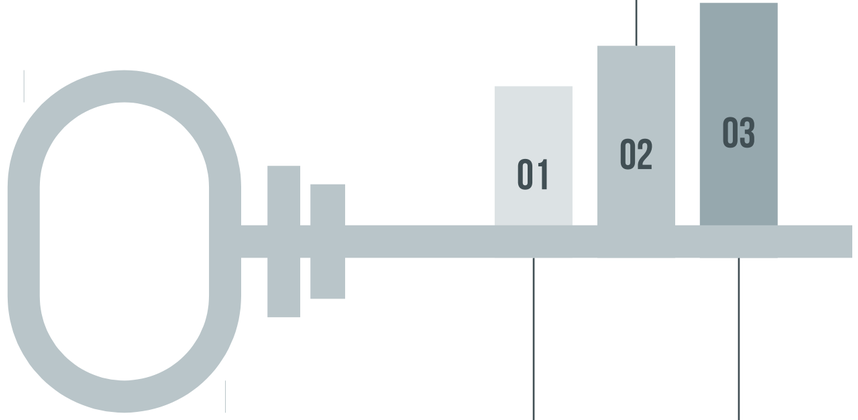
PASO 1: INSTALAR/EJECUTAR

```
$ sudo apt-get install clamav clamav-daemon clamtk
$ clamtk&
```

PASO 3: ANÁLISIS

- Analizar carpeta.

3 GESTOR DE CONTASEÑAS
KEEPASS



PASO 1: INSTALAR

```
$ sudo add-get-repository ppa:jtaylor/keepass
$ sudo apt-get install keepass2
$ sudo apt-get install xdotool
```

PASO 2: PREPARATIVOS

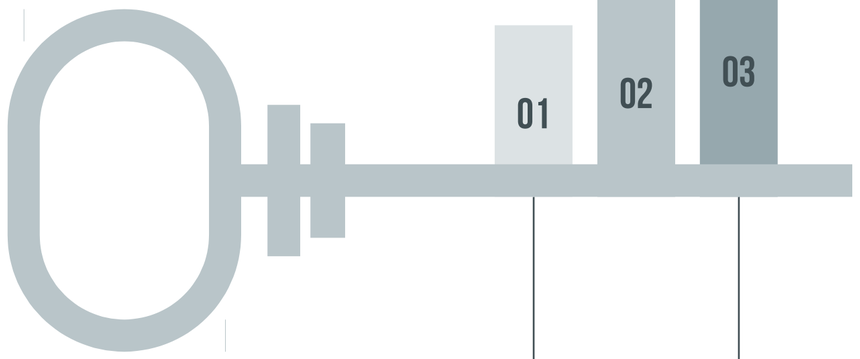
Crear base de datos con contraseña maestra..

- Contraseña fuerte, ej. método PAO (Persona-Accion-Objeto)

PASO 3: REGISTRO DE CLAVES

- Añadir registro: usuario, clave, URL servicio
- Abrir la URL
- Realizar auto-rellenado

4 ACTUALIZACIONES DE SOFTWARE



PASO 1: INSTALAR

No requiere ninguna instalación adicional de programas

PASO 2: AUTOMÁTICA

“Software y actualizaciones”:
- Comprobar que esta configurado para que se realiza de forma automática.
- Comprobar repositorios

PASO 3: MANUAL

$ sudo apt update && sudo apt dist-upgrade
$ sudo do-release-upgrade

05

PRIVACIDAD

1 NAVEGACIÓN PRIVADA

Navegación privada, noscript o Ghostery.

2 METADATOS

Exiftool.

3 CIFRADOS DE DATOS

Cifrar unidades extraibles.

1 NAVEGACIÓN PRIVADA

Menú navegador → Nueva ventana privada

PESTAÑA PRIVADA

01

02

03

NOSCRIPT

El contenido activo se ejecute solo desde los sitios de confianza, y protéjase contra XSS y los ataques Clickjacking, "Spectre", "Meltdown" y otros exploits de JavaScript.

GHOSTERY

Bloquea anuncios, detiene rastreadores y acelera sitios web.

2 LIMPIEZA DE METADATOS

Exiftool:

```
$ sudo apt-get libimage-exiftool-perl
```

INSTALACIÓN

01

VER METADATOS

02

```
$ exiftool imagen.jpg
```

LIMPIEZA

03

Todos:

```
$ exiftool -all= imagen.jpg
```

3 CIFRADO DE DISPOSITIVOS

Seleccionar “Discos” en el grupo “Utilidades”

UTILIDAD “DISCOS”

01

02

03

FORMATEAR USB

- Opciones adicionales de partición → Formatear partición → Volumen protegido por contraseña (LUKS)

USO

Al montar el volumen nos pedirá la contraseña, a partir de lo cual trabajamos de forma normal.

THANK YOU!

ALGUNA CUESTIÓN?

Seguridad y Privacidad con fuentes abiertas