LiveCD VPNRDP

Guía de configuración de un sistema operativo autoarrancable para trabajar en modalidad no presencial (Teletrabajo)

Proyecto: LiveCD VPNRDP (DigitalizaAAPP)
Documento: vpnrdp_kiosk_v00r03.odt
Versión: v00r03
Fecha: 23/01/2021 19:34
Repositorio: https://github.com/digitaliza-aapp/vpnrdp
Licencia: GNU General Public License v3.0

Control de cambios

Versión	Fecha	Descripción	Responsable
00r00	21/03/20	Versión inicial	Felipe Muñoz Brieva
00r02	25/03/20	Ajustes y corrección de errores	FMB[1]
00r03	23/01/21	Imagen USB	FMB

Sumario

1 FMB: Felipe Muñoz Brieva

Ausencia de garantías.
EL LIVECD VPNRDP SE PROVEE EN SU ESTADO ACTUAL Y SIN GARANTÍAS DE NINGÚN TIPO. NO SE OFRECE DE MANERA EXPLÍCITA, IMPLÍCITA, NI JURADA GARANTÍAS, AFIRMACIONES NI DECLARACIONES DE NINGÚN TIPO CON RESPECTO AL LIVECD VPNRDP.

Descargo de responsabilidad.
Usted recibe el LIVECD VPNRDP de forma gratuita. POR CONSIGUIENTE, USTED RECONOCE Y ACEPTA QUE EL PERSONAL QUE HA PARTICIPADO EN EL PROYECTO NO TENDRÁ RESPONSABILIDAD ALGUNA QUE SURJA DEL USO DEL LIVECD O SE RELACIONE CON DICHO USO. SU ÚNICO DERECHO O RECURSO LEGAL ANTE CUALQUIER PROBLEMA O DISCONFORMIDAD CON EL LIVECD VPNRDP ES DEJAR DE USARLO DE INMEDIATO.

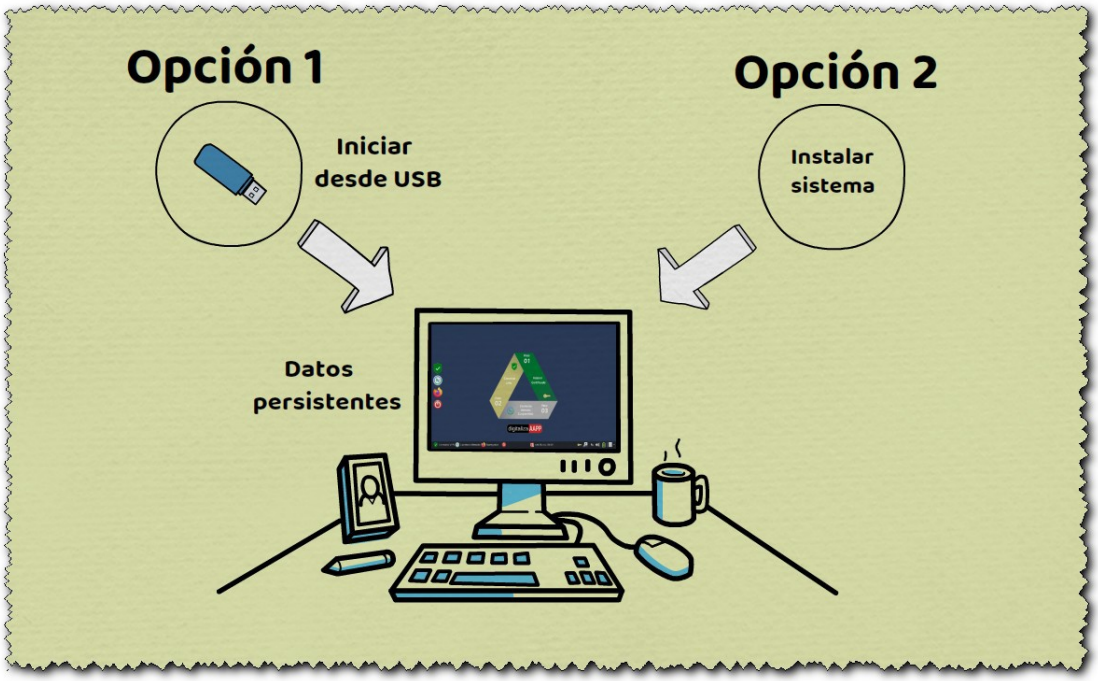
Disclaiming warranty
LIVECD VPNRDP IS PROVIDED IN ITS CURRENT STATUS AND WITHOUT WARRANTIES OF ANY KIND. NO WARRANTIES, CLAIMS, OR STATEMENTS OF ANY KIND WITH REGARD TO THE LIVECD VPNRDP ARE PROVIDED EXPLICIT, IMPLIED, OR SWORN.

Limiting liability
You receive LIVECD VPNRDP for free. ACCORDINGLY, YOU ACKNOWLEDGE AND AGREE THAT THE PERSONNEL WHO HAVE PARTICIPATED IN THE PROJECT SHALL HAVE NO LIABILITY ARISING FROM THE USE OF THE LIVECD OR RELATING TO SUCH USE. YOUR SOLE RIGHT OR LEGAL REMEDY FOR ANY PROBLEM OR DISPUTE WITH THE LIVECD VPNRDP IS TO STOP USING IT IMMEDIATELY.

1 Introducción

Bring your own device es una política empresarial consistente en que los empleados utilicen sus dispositivos para tener acceso a recursos corporativos. Al utilizar dispositivos propios se puede hacer uso de software que puede no ser el recomendado por la empresa y el comportamiento de estos usuarios puede escaparse del control del departamento de IT[2]. Una posible solución es el uso de sistemas operativos autoarrancables (*LiveCD*[3]) desarrollados por la empresa.

A continuación se detalla el proceso de configuración de un sistema basado en una distribución ligera *Linux* , basada en el sistema operativo *Ubuntu,* para realizar conexiones seguras sobre redes públicas mediante *VPN*[4] a escritorios corporativos remotos utilizando el protocolo *RDP*[5].



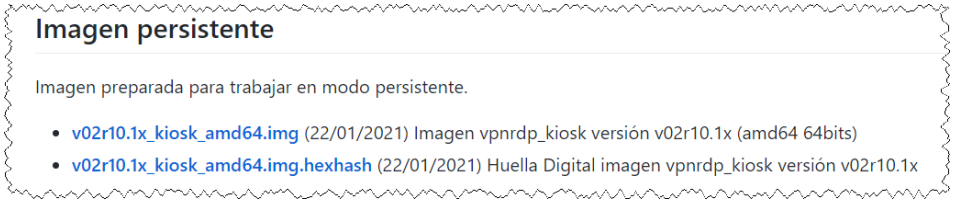
2 IT: Information Technology – Departamento de Tecnologías de la Información
3 LiveCD: Sistema operativo almacenado en un CD/DVD/USB que puede ser ejecutado sin que haya necesidad de instalarlo en el disco duro
4 VPN: Virtual Private Network – Red Privada Virtual
5 RDP: Protocolo de Microsoft para la comunicación en la ejecución de una aplicación entre un terminal y un servidor Windows

Para realizar la conexión existen unos requisitos previos[6]:

- *VPN* activa para conectar mediante el sistema VPNRDP
- *Certificado Digital* válido exportado con clave privada (extensión *pfx* ó *p12*) grabado en pendrive
- URL ó dirección IP para acceder a la VPN
- Usuario de la VPN
- IP del equipo corporativo
- Usuario del equipo corporativo (dominio)
- Nombre del dominio
- Contraseñas del:
  - Certificado digital
  - Correo electrónico
  - Usuario del dominio

2 Preparar pendrive autoarrancable

La opción recomendada para preparar un pendrive *(USB)* autoarrancable con el sistema *VPNRDP* es a partir del fichero con la imagen persistente



https://github.com/digitaliza-aapp/vpnrdp

ya que permite el arranque dual *BIOS (MBR)* y *UEFI*, está preparada para trabajar en modo persistente (no es necesario instalar el certificado en cada arranque del sistema) y crea una partición para poder almacenar el certificado digital (*pfx* ó *p12*) y facilitar su instalación.

La imagen puede ser instalada en el pendrive mediante programas como Rufus (https://rufus.ie/)

Para tener una buena experiencia de uso con el sistema se recomienda utilizar pendrives *USBs 3.0* que proporcionen un buen rendimiento en transferencia de archivos para lectura y escritura. En las pruebas se ha utilizado un modelo con velocidad de hasta 150 MB/s de lectura/escritura (*Sandisk Ultra Flair Memoria Flash USB 3.0 de 32 GB*).

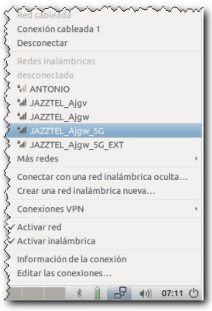
3 Arranque y configuración del sistema operativo

1. Con el ordenador apagado conectar el *USB* a uno de los puertos libres ó introducir el *DVD* en el lector, encender el equipo y acceder al menú de arranque[7] presionando la tecla definida por el fabricante (Ver *Anexo I: Teclas para acceder al menú de arranque*)

6 Consultar requisitos previos al Departamento de Informática
7 Menú de arranque: Boot Menu

2. Seleccionar la unidad USB en el menú de arranque para iniciar el sistema.

Una vez iniciado el sistema si la conexión a *internet* se va a realizar por Wifi debe seleccionar una red activa para conectar a internet.



Nota:

Las redes activas se pueden seleccionar mediante el icono que aparece en la zona inferior derecha 

Para configurar el acceso al *Escritorio Remoto Corporativo* deben realizarse 3 pasos:

Paso 1. Instalar certificado

Iniciar el instalador mediante el icono:

pulsar sobre el botón ***Instalar***

conectar el *pendrive* con el *Certificado Digital,* ***Continuar*** , seleccionar el fichero con el certificado

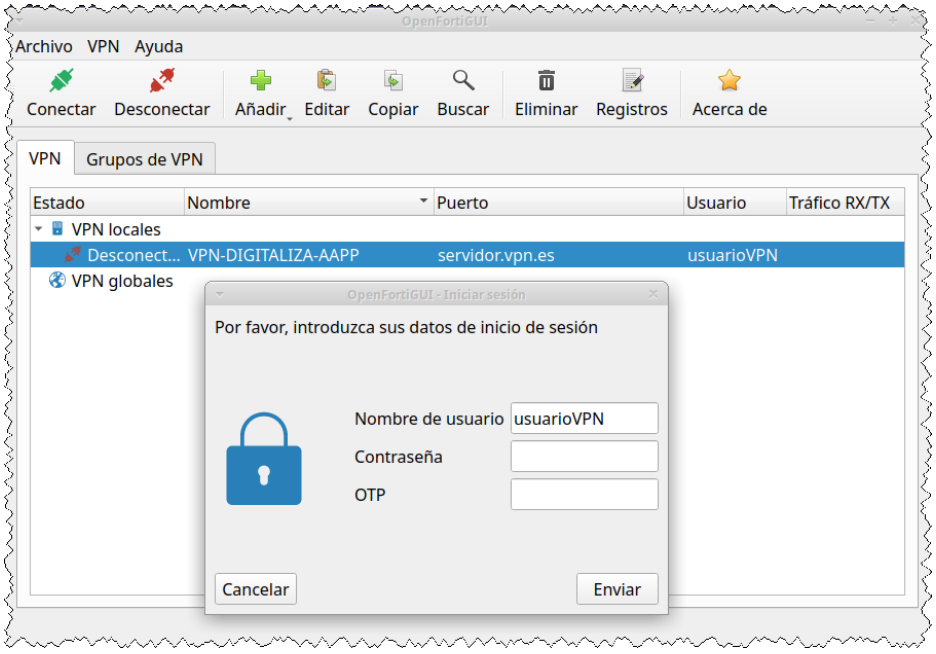
y completar los datos del formulario:

Pulsar el botón ***Aceptar*** para finalizar la instalación del certificado.

Paso 2. Conectar mediante VPN

Conectar a la VPN haciendo doble clic sobre el icono ***Conexión VPN***

seleccionar sobre la línea *Desconectado... VPN-DIGITALIZA-AAPP* y pulsar en el botón ***Conectar***



teclear ***Contraseña*** y pulsar el botón ***Enviar*** (el campo OTP debe dejarse en blanco).

si los datos son correctos transcurridos unos segundos aparecerá ***Conectado***

Paso 3. Conectar al equipo corporativo remoto

Conectar con el *Escritorio Corporativo Remoto* seleccionando el icono

hacer doble clic con el ratón sobre la línea *Escritorio Remoto Corporativo*

y proporcionar los datos de autenticación para realizar la conexión

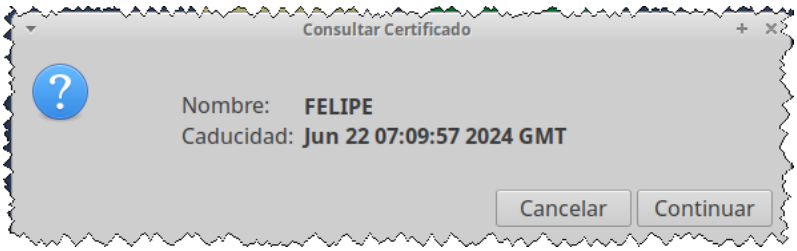
Puede expandirse la pantalla para ocupar todo el área de pantalla disponible mediante los botones:

Borrar datos personales del equipo

Iniciar el programa mediante el icono:

pulsar sobre el botón ***Borrar*** para eliminar todos los datos personales del equipo (certificado digital, usuario, etc.)

Mediante el botón ***Consultar*** es posible ver la fecha de caducidad del certificado

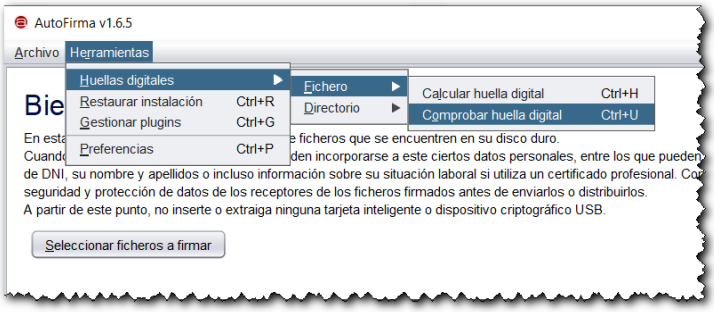


Anexo I: Teclas para acceder al menú de arranque

Fabricante	**Tecla que debe presionar para arrancar el sistema**
Acer	Escape, F9 ó F12
AsRock	F11
Asus	Escape ó F8
Biostar	F9
Compaq	Escape ó F9
Dell	F12
eMachines	F12
Evga	F7
FoxConn	F7
Gigabyte	F12
HP	Escape ó F9 (En algunos casos es necesario Escape y después F9)
Intel	F10
Lenovo	F8, F10, F11 ó F12
Msi	F11
Nec	F5
Optima	F11
Packard Bell	F8
Samsung	Escape o F12
Sharp	F2
Sony	F10 ó F11
TicNova	F11
Toshiba	F12
Ttl	F11
Zotac	Esc

Anexo II: Comprobar Huella digital de imagen ISO descargada

Mediante AutoFirma[8] puede comprobarse la Huella Digital de la imagen ISO



8 AutoFirma: Aplicación de firma electrónica desarrollada por el Ministerio de Hacienda y Administraciones Públicas https://firmaelectronica.gob.es/Home/Descargas.html

Anexo III: Créditos

El *LiveCD vpnrdp* utiliza componentes *Open Source*. A continuación puede encontrar un enlace a los proyectos. Reconocemos y agradecemos a los desarrolladores su contribución al código abierto.

This application uses *Open Source* components. You can find a link to their projects , we acknowledge and are grateful to these developers for their contributions to open source.

Software	**URL**	**Descripción**
LiveCD vpnrdp	https://github.com/digitaliza-aapp/vpnrdp	LiveCD - Conexión a escritorios mediante VPN y RDP
Xubuntu	https://xubuntu.org/ https://wiki.ubuntu.com/Xubuntu	Distribución Linux ligera basada en Ubuntu
OpenfortiGui	https://github.com/theinvisible/openfortigui https://apt.iteas.at/	*VPN-GUI* para conexiones a *Fortigate* basado en *openfortivpn*
Remmina	https://remmina.org/	Cliente de escritorio remoto
Mkusb	https://launchpad.net/~mkusb/+archive/ubuntu/ppa	Herramienta para crear unidades de arranque USB
Clamav	https://www.clamav.net/downloads	Antivirus Open Source
Firefox	http://mozilla.org	Navegador Web
FreeRDP	https://github.com/FreeRDP/FreeRDP	Implementación protocolo RDP
XFreeRDP-GUI	https://github.com/wyllianbs/xfreerdp-gui	Entorno gráfico para FreeRDP
Docky	https://launchpad.net/docky	Lanzador de aplicaciones
Systemback	https://sourceforge.net/projects/systemback/	Simple system backup and restore