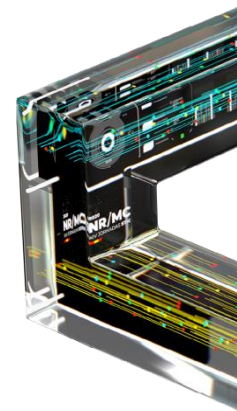


#XIVJORNADASCCNCERT

**“Estado de Alarma.
LA HORA MÁS OSCURA”**





Antonio Grimaltos Vidal

***Oficina de seguridad de la Información.
Consellería de Sanidad Universal y
Salud Pública.***

GENERALITAT VALENCIANA
grimaltos_ant@gva.es



Gloria Tamayo

***Enterprise Account Manager Administración
Pública***

Cytomic

gloria.Tamayo@cytomic.ai

Innovación en ciberseguridad_

80% -> innovación de los atacantes

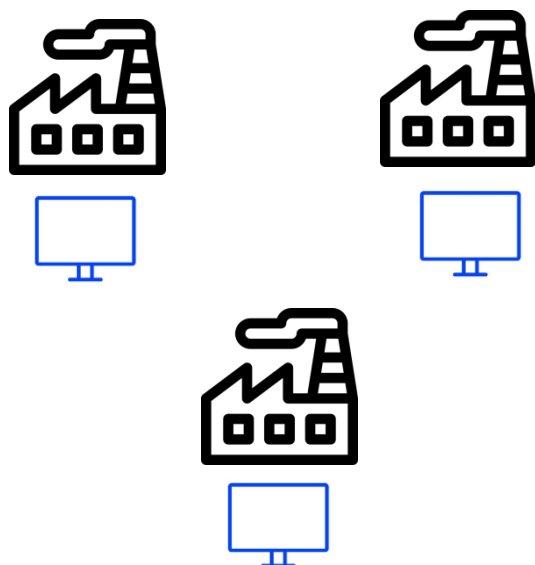
20% -> cambios en el entorno

80% -> cambios en el entorno

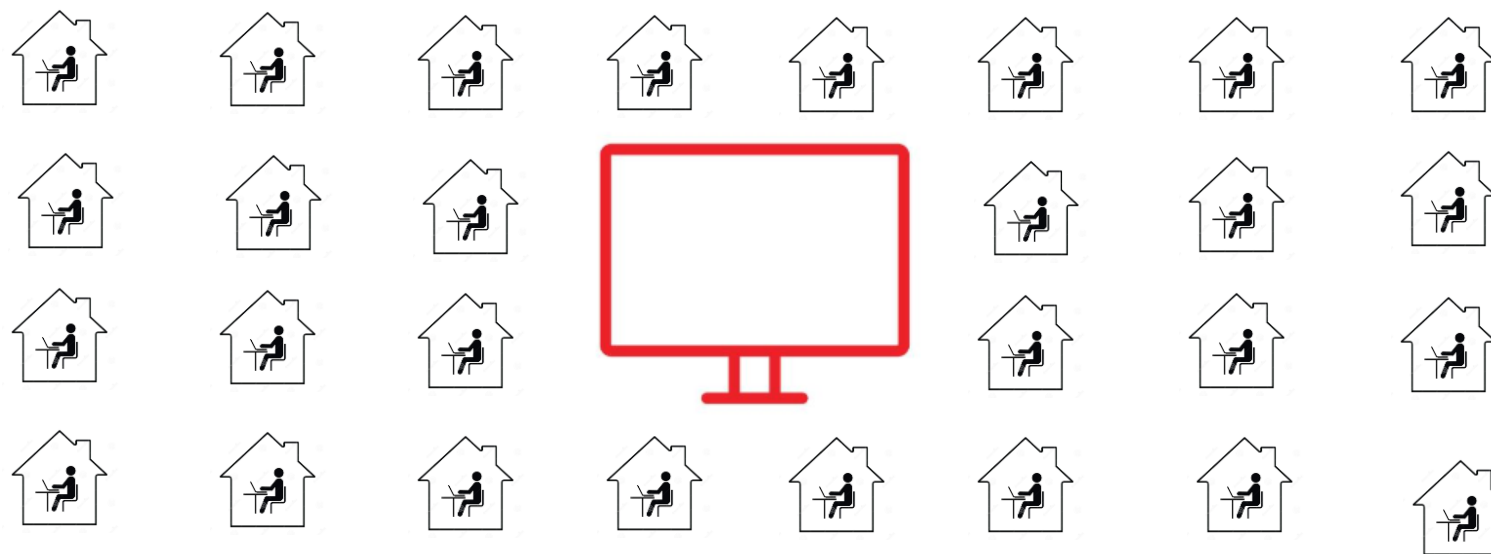
20% -> innovación de los atacantes

La nueva organización_

X oficinas – XXXX empleados



XXXX oficinas

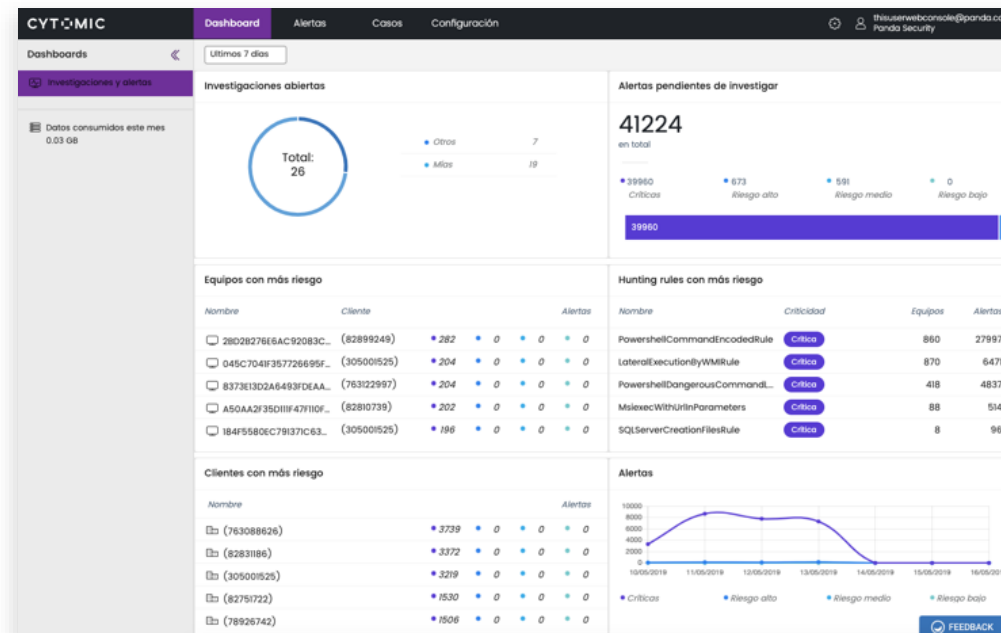




Researchers warn of a seven-fold rise in ransomware attacks compared with last year alone - and attackers are continually evolving their tactics.

Cytomic_

- Visibilidad y gestión remota.
- Zero Trust Application Service.
- Threat Hunting Service.



La hora más oscura

4 de junio de 1940

... Llegaremos hasta el final, lucharemos en Francia,
lucharemos en los mares y océanos, lucharemos en el aire,
defenderemos nuestra isla, cualquiera que sea el costo,
lucharemos en las playas, lucharemos en las pistas de
aterrizaje, lucharemos en los campos y en las calles,
lucharemos en las colinas, ¡nunca nos rendiremos!...

Winston Churchill, primer ministro británico
de 1940 a 1945 y de 1951 a 1955

La hora más oscura

6 de marzo de 2020



USO OFICIAL



CCN-CERT – Medidas de seguridad para el acceso remoto

Abstract: Garantizar la seguridad de los sistemas de información involucrados en los accesos remotos por si se activan medias de contención o de teletrabajo excepcionales. En la actualidad existen múltiples campañas de *ransmoware* activas y dado que las conexiones remotas pueden ser una vía de entrada de malware o personas no identificadas a los sistemas, se desarrolla en este documento una breve explicación de medias complementarias a cada organismo en sus accesos remotos.

La hora más oscura

6 de marzo de 2020

3.2 Equipos portátiles corporativos

Debe considerarse la primera forma de acceso, al contemplar las medidas de seguridad del organismo. Aunque deben cumplir las siguientes medidas:

- Tener las últimas actualizaciones de sistemas operativo instalada
- Aplicaciones ofimáticas, lectores de pdf y de uso cotidiano, actualizadas a la última versión de parches de seguridad
- Tener antivirus instalado
- Estado del antivirus actualizado como sugerencia al día de conectar, en caso de no poderse al menos tres (3) días antes.
- Se sugiere tener Endpoint instalado.

3.3 Equipos personales

Estos pueden ser los equipos más vulnerables. Por ello, es la última opción de conectividad. Dado el caso de su utilización, se deben aplicar las medidas anteriores y además ponerlo en conocimientos de los equipos de seguridad del organismo por si se deben establecer medidas adicionales a las establecidas.



24 Departamentos de salud

29 Hospitales

37 CPD'S

1.100 Servidores

35.000 Equipos de usuario

24 Departamentos de salud

29 Hospitales

37 CPD'S

DENTRO DE NUESTRA RED ESTAMOS SEGUROS

1.100 Servidores

35.000 Equipos de usuario



DENTRO DE NUESTRA RED LAS PROTECCIONES SIGUEN FUNCIONANDO

24 Departamentos de salud

29 Hospitales

37 CPD'S

1.100 Servidores

35.000 Equipos de usuario

La hora más oscura

10 de marzo de 2020

Medida de protección frente al COVID

TELETRABAJO

- 1500 A 1800 TRABAJADORES DESDE SU CASA, CON SUS EQUIPOS PROPIOS YA QUE NO DISPONEMOS DE ESA CANTIDAD DE EQUIPOS PORTÁTILES

PROBLEMAS

- CONEXIÓN POR VPN A LAS APLICACIONES DE CONSELLERIA O A SU ESCRITORIO REMOTO
- IMPACTO QUE PRODUCIRÍAN ESOS EQUIPOS CONECTÁNDOSE TAL Y COMO ESTAN EN SU ENTORNO FAMILIAR.

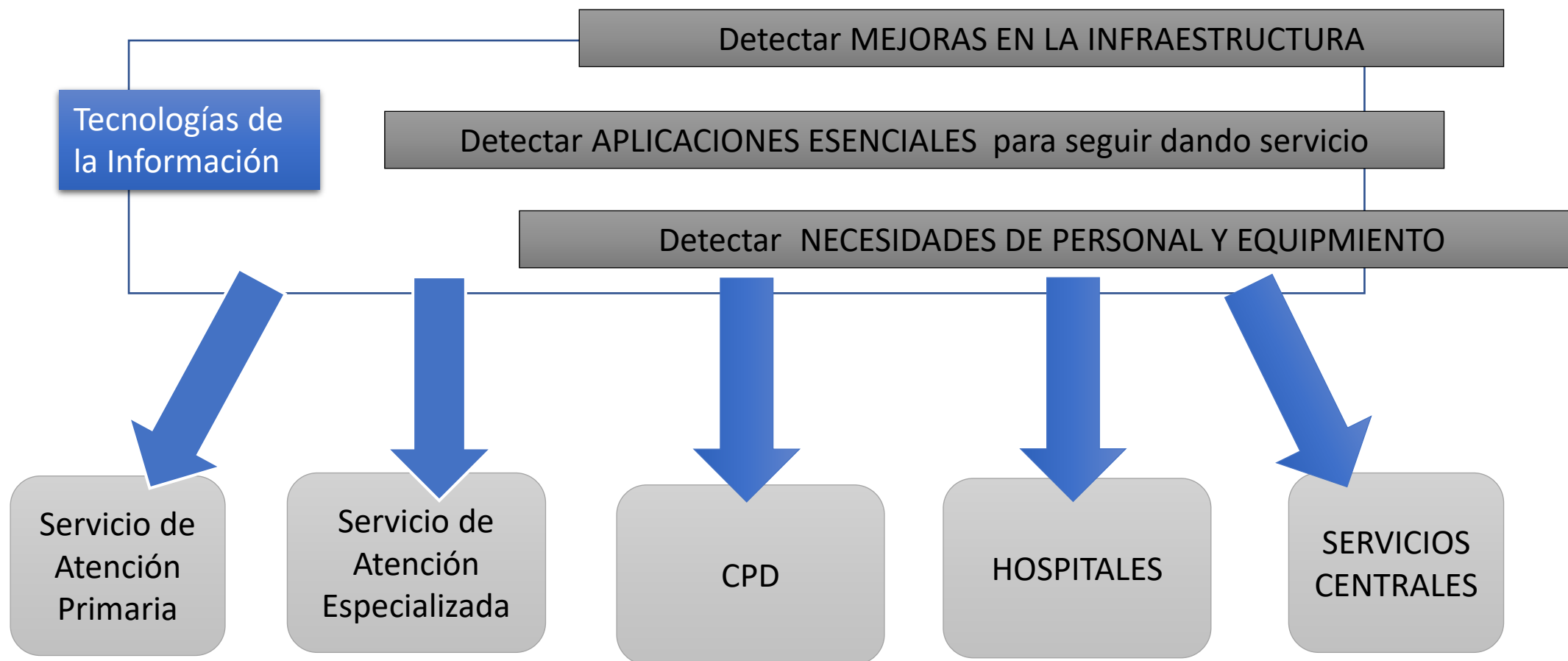
ASÍ QUE,

¿CÓMO GARANTIZAMOS QUE ESOS EQUIPOS QUE SE CONECTARÁN AL ENTORNO DE CONSELLERÍA ESTARÁN LIMPIOS O PRODUCIRÁN EL MENOR IMPACTO POSIBLE?

La hora más oscura

10 de marzo de 2020

TELETRABAJO



La hora más oscura

11 de marzo de 2020

MEJORAS NECESARIAS EN LA INFRAESTRUCTURA

SERVIDOR DE VPN

TARJETA
RED
+
Capacidad

SONDA IDS

TARJETA
RED
+
Capacidad

La hora más oscura

11 de marzo de 2020

APLICACIONES ESENCIALES para seguir dando servicio

CA/SIGESTI

Aplicación para comunicación y
resolución de Incidencias

INTRANET

POSIBILIDAD DE PUBLICARLA EN INTERNET

- ANALISIS DE RIESGOS
- AUDITORIA DE Csirt-CV

TELETRABAJANDO SEGUIR ATENDIENDO INCIDENCIAS

La hora más oscura

11 de marzo de 2020

APLICACIONES ESENCIALES para seguir dando servicio

CA/SIGESTI

Aplicación para comunicación y
resolución de Incidencias

INTERNET

- SUBIMOS LA VERSIÓN DE APACHE
- BLOQUEAMOS CONEXIONES DESDE EL EXTERIOR DE ESPAÑA
- VALORAMOS LA POSIBILIDAD DE QUE SE EXPLOTARAN VULNERABILIDADES CONOCIDAS DE LA APLICACIÓN
- EVALUAMOS EL IMPACTO QUE PRODUCIRÍAN
- NOS LA JUGAMOS

ASÍ AUNQUE LOS OPERADORES ESTIVIESEN
TELETRABAJANDO PODRÍAN SEGUIR ATENDIENDO
INCIDENCIAS

La hora más oscura

11 de marzo de 2020

APLICACIONES ESENCIALES para seguir dando servicio

Certificados de Servidor y de
Aplicación a punto de caducar

LISTA DE CERTIFICADOS A CADUCAR EN UN MES.

Para tener previsto como renovar esos certificados
aunque estuviésemos en remoto



24 Departamentos de salud

29 Hospitales

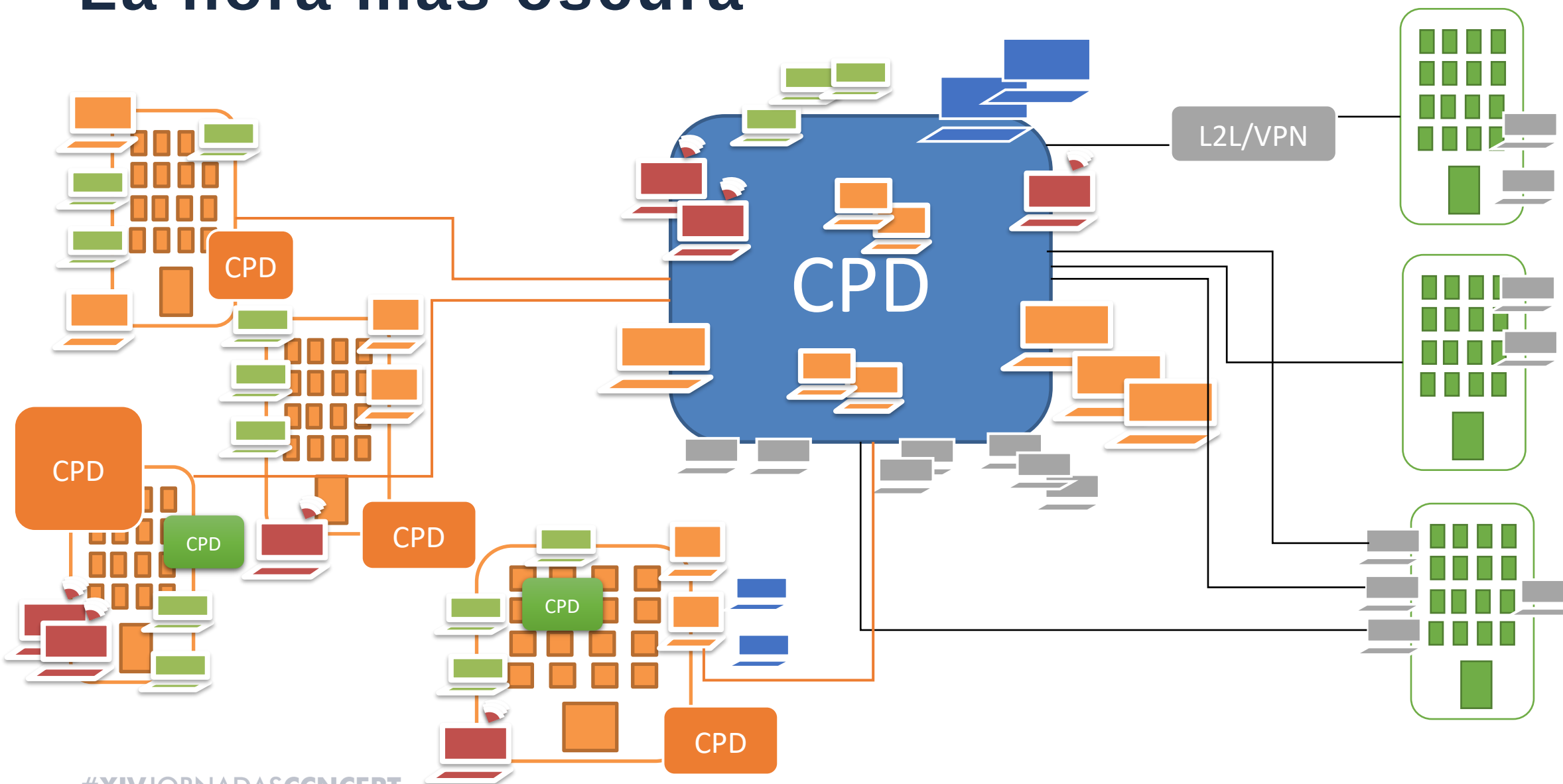
37 CPD'S

1.100 Servidores

35.000 Equipos de usuario

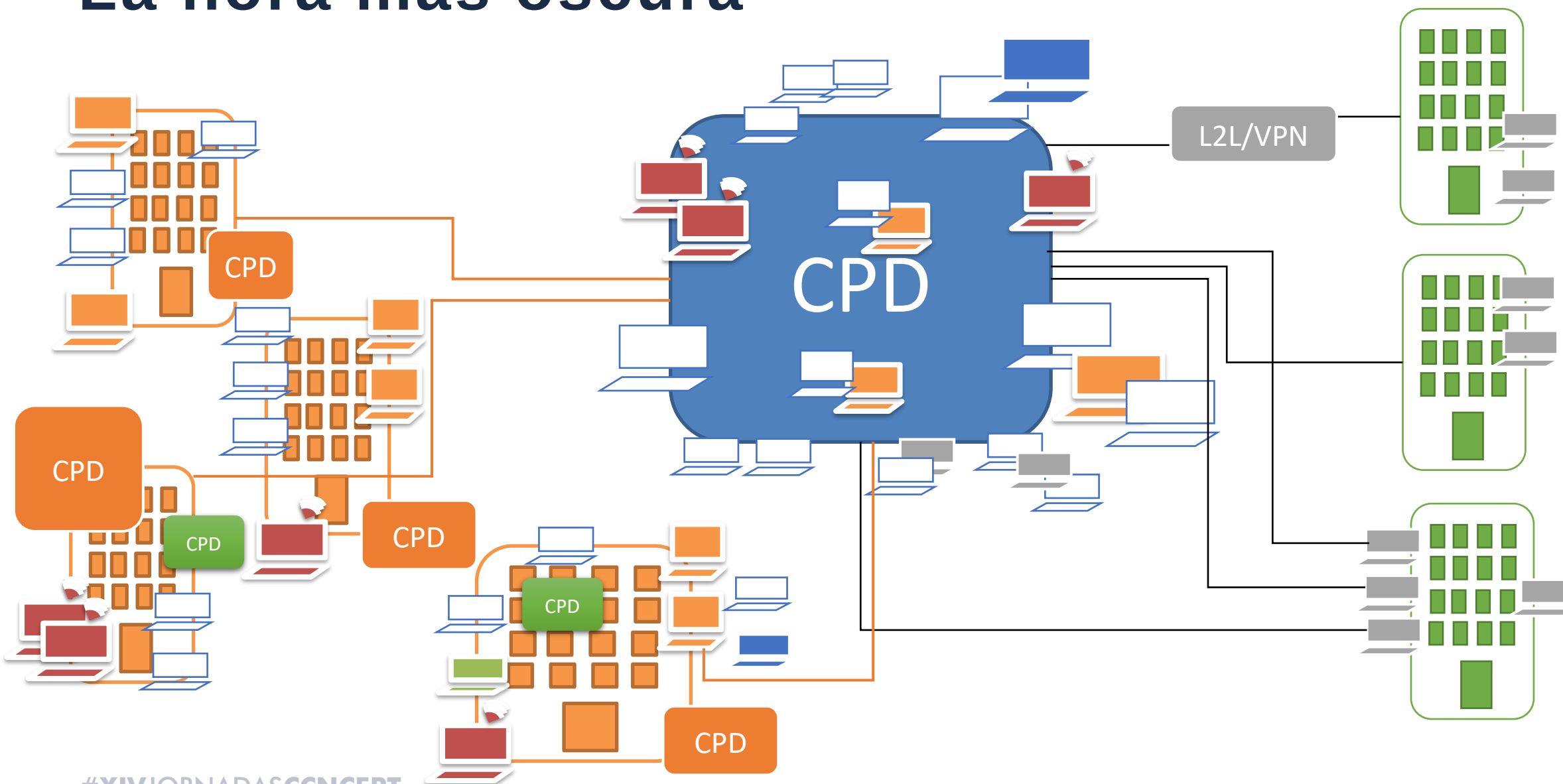
La hora más oscura

NECESIDADES DE PERSONAL Y EQUIPAMIENTO



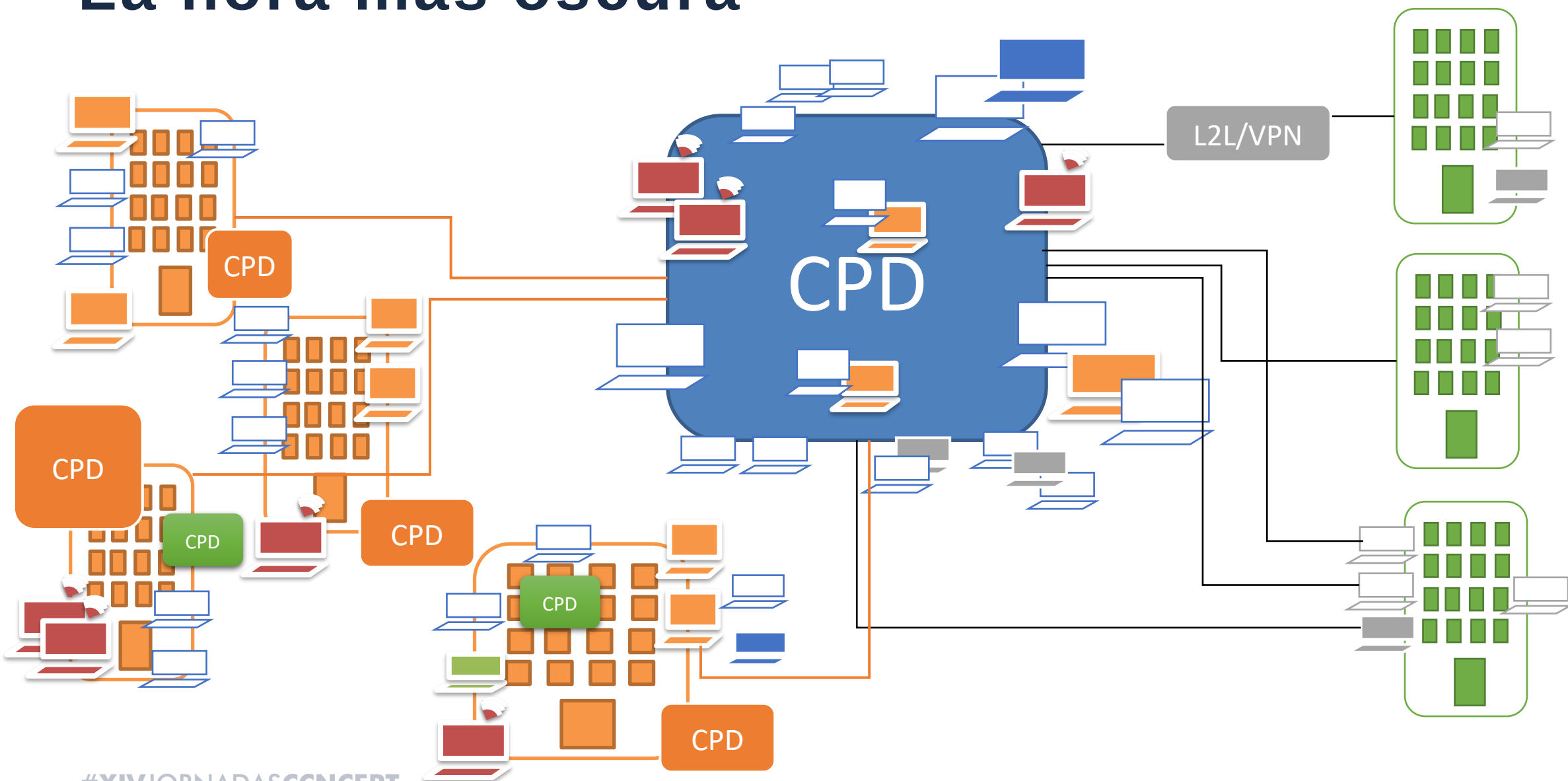
La hora más oscura

NECESIDADES DE PERSONAL Y EQUIPAMIENTO



La hora más oscura

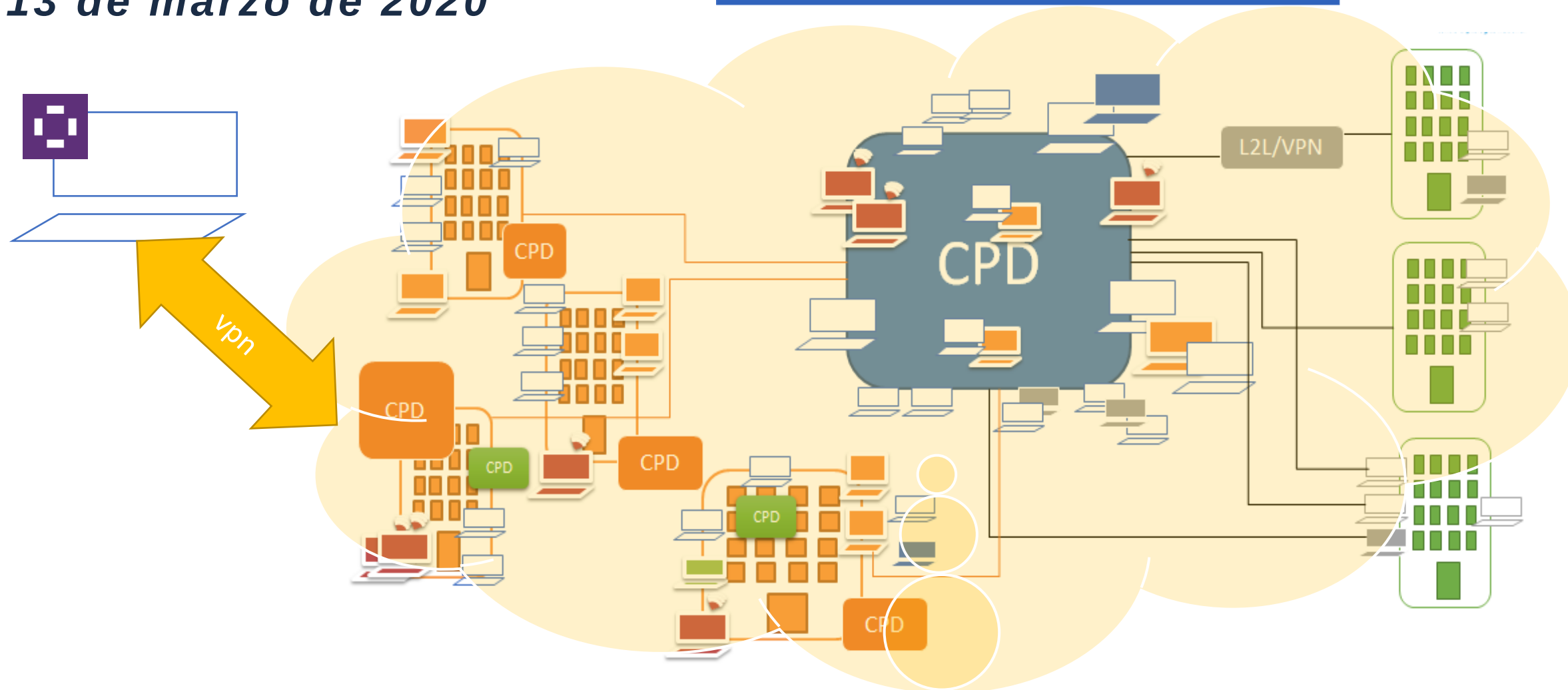
NECESIDADES DE PERSONAL Y EQUIPAMIENTO



La hora más oscura

13 de marzo de 2020

EMPEZAMOS A DESPLEGAR LA SOLUCIÓN



Seguimiento.

De: Gloria Tamayo <gloria.tamayo@cytomicmodel.com>

Para: Vicente [REDACTED]

CC: [REDACTED]

Asunto: RE: Licencias Temporales

Enviado el: vi. 13/03/2020 15:32

Buenas tardes Vicente,
Ya he contactado con Antonio. Nos ponemos a ello.
Saludos,
Gloria

De: [REDACTED]

Enviado el: viernes, 13 de marzo de 2020 15:07

Para: Gloria Tamayo <gloria.tamayo@cytomicmodel.com>

Asunto: RE: Licencias Temporales

Hola Gloria.

Agradecemos mucho vuestro ofrecimiento para ayudarnos en esta situación de crisis del Covid-19.

Por favor, contacta con Antonio, o el contactará contigo para que podamos hacer uso de las licencias temporales gratuitas que nos ofrecéis.

Saludos.

La hora más oscura

13 de marzo de 2020

- CONTROL CENTRALIZADO
- PERMITE CONFIGURAR LA **PRIVACIDAD**
 - No guardamos datos del usuario solo la ip (de conexión)
- UTILIDADES DE LA CONSOLA PARA CONFIGURAR
- UTILIDADES DE LA CONSOLA PARA INVESTIGAR
- POSIBILIDAD DESDE LA CONSOLA DE CONECTARSE A LOS SERVIDORES DE PANDA
- POSIBILIDAD DE LIMITAR LAS RECONEXIONES
- POSIBILIDAD DE CONTROLAR LA DESINSTALACIÓN DE PANDA
 - Importantísimo: se autorizaba la desinstalación si se ha desinstalado el software de VPN

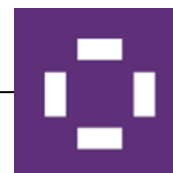


Certificada para el ENS Nivel ALTO

- **LEGAL**
- **NOTIFICA LOS EQUIPOS**
- **WINDOWS, MAC Y LINUX**

La hora más oscura

Configurar la PRIVACIDAD



- PERMITE CONFIGURAR LA **PRIVACIDAD**. No guardamos datos del usuario solo la ip (de su router) y el nombre del equipo.
- UTILIDADES DE LA CONSOLA PARA CONGIGURAR DIFERENTES GRUPOS

Conselleria de Sanitat – Configuración externos

La configuración que se ha establecido se ha atendido principalmente a equilibrar la protección con los problemas que puedan afectar a la privacidad y a posibles protecciones que el usuario ya tenga disponible en su máquina.

La configuración se divide en varias partes atendiendo a diferentes cuestiones:

- **Ajustes por equipo:** Referente a actualizaciones y contraseña para que no se pueda desinstalar la protección localmente.
- **Configuración de red:** Configuración de idioma y otras consideraciones necesarias cuando estamos en una red empresarial, que no es el caso.
- **Estaciones y servidores:** Configuración referente a la protección.

Ajustes por equipo

Se ha definido una única configuración llamada **Externos**



Nombre	Fecha de modifica...	Tipo
 CCN-CERT_BP-18 Recomendaciones para Teletra...	19/03/2020 1:23	Adobe Acrobat D...
 BYOD VPN CYTOMIC.docx	19/03/2020 1:45	Documento de Mi...
 Conselleria de Sanitat - Configuración externos.do...	19/03/2020 2:31	Documento de Mi...
 BYOD VPN CYTOMIC v1.1.docx	20/03/2020 11:08	Documento de Mi...
 BYOD VPN CYTOMIC v1.1 revDPD sin cookies.docx	20/03/2020 19:43	Documento de Mi...
 Anexo1 Instalacion Cytomic.docx	27/03/2020 11:44	Documento de Mi...
 Anexo1 Instalacion Cytomic.pdf	27/03/2020 11:45	Adobe Acrobat D...
 Fwd CCN-CERT Aviso CiberCOVID19 nueva sec...	01/04/2020 0:04	Elemento de Outl...
 Informe_del_Archivo_document (1).pdf_(28f28eea...	04/04/2020 21:02	Adobe Acrobat D...

La hora más oscura

Condiciones de uso

Condiciones para el uso de equipos domésticos durante la situación de emergencia generada por COVID-19

Las tecnologías de la información y las comunicaciones (TIC) son elementos críticos para la actividad de los centros sanitarios, así como para la coordinación de todo el sistema público de salud. Los profesionales que se ocupan de esas tecnologías son otro elemento crítico. Su conocimiento sobre las infraestructuras y servicios TIC de cada centro les hace difícilmente reemplazables.

En las circunstancias excepcionales en que nos encontramos es preciso evitar la exposición del personal a riesgos innecesarios que pudieran comprometer su salud y la operatividad de los centros sanitarios. Esta situación obliga a considerar medidas extraordinarias, como permitir a determinadas personas el acceso desde sus domicilios a determinados sistemas de información de la Conselleria para realizar funciones análogas a las que realizan desde sus puestos de trabajo habituales (teletrabajo). Es más, ante la posibilidad de que los equipos corporativos disponibles no fueran suficientes para atender toda la demanda, se plantea la cuestión de si se podría permitir dicho acceso desde equipos personales (=domésticos), y en tal caso bajo qué condiciones.¹

El uso de equipos domésticos para el acceso a infraestructuras, sistemas o información bajo la responsabilidad de la Conselleria entraña riesgos para todos los agentes implicados. En términos generales esos riesgos son inasumibles.

Nombre	Fecha de modifica...	Tipo
 CCN-CERT_BP-18 Recomendaciones para Teletra...	19/03/2020 1:23	Adobe Acrobat D...
 BYOD VPN CYTOMIC.docx	19/03/2020 1:45	Documento de Mi...
 Conselleria de Sanitat - Configuración externos.do...	19/03/2020 2:31	Documento de Mi...
 BYOD VPN CYTOMIC v1.1.docx	20/03/2020 11:08	Documento de Mi...
 BYOD VPN CYTOMIC v1.1 revDPD sin cookies.docx	20/03/2020 19:43	Documento de Mi...
 Anexo1 Instalacion Cytomic.docx	27/03/2020 11:44	Documento de Mi...
 Anexo1 Instalacion Cytomic.pdf	27/03/2020 11:45	Adobe Acrobat D...
 Fwd CCN-CERT Aviso CiberCOVID19 nueva sec...	01/04/2020 0:04	Elemento de Outl...
 Informe_del_Archivo_document (1).pdf_(28f28eea...	04/04/2020 21:02	Adobe Acrobat D...

La hora más oscura

Procedimiento de Instalación

ANEXO 1. Instalación del agente Cytomic Endpoint Agent

Los siguientes enlaces le permitirán descargar el instalador en su equipo. Una vez descargado tendrá que ejecutarlo (doble click) para proceder a su instalación. A partir de ese momento el programa estará activo y arrancará automáticamente cada vez que encienda el equipo. Para elegir el instalador adecuado dispone de varias opciones:

Si tiene usuario y cuenta del dominio CS (los que usa para identificarse cuando enciende un equipo de la Conselleria)

1. En equipos con Windows:
<https://transit.san.gva.es/owncloud/index.php/s/Ta0HIAV8V2wsLTh>
2. En equipos con MacOS:
<https://transit.san.gva.es/owncloud/index.php/s/9XB2EnGMpGya82f>
3. En equipos con Linux:
<https://transit.san.gva.es/owncloud/index.php/s/UdVYCqR0zxcueeY>

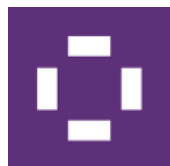
En caso contrario, o si hubiera tenido alguna dificultad con el anterior:

1. En equipos con Windows:
<https://manage.cytomicmodel.com/api/v1/accounts/8dcd781b-068e-4c3f-b6b0-9246dc69e613/sites/a3c25366-c340-41d4-9805-4e8d8075fc63/installers?installerType=2&platform=1&managedConfigurationId=106815ce-6fb6-4efa-9b09-e2cb309f7444&customGroupId=5a00c15a-2dd8-42cb-9abe-89e812cb8b05&integrationGroupType=0>

Nombre	Fecha de modifica...	Tipo
 CCN-CERT_BP-18 Recomendaciones para Teletra...	19/03/2020 1:23	Adobe Acrobat D...
 BYOD VPN CYTOMIC.docx	19/03/2020 1:45	Documento de Mi...
 Conselleria de Sanitat - Configuración externos.do...	19/03/2020 2:31	Documento de Mi...
 BYOD VPN CYTOMIC v1.1.docx	20/03/2020 11:08	Documento de Mi...
 BYOD VPN CYTOMIC v1.1 revDPD sin cookies.docx	20/03/2020 19:43	Documento de Mi...
 Anexo1 Instalacion Cytomic.docx	27/03/2020 11:44	Documento de Mi...
 Anexo1 Instalacion Cytomic.pdf	27/03/2020 11:45	Adobe Acrobat D...
 Fwd CCN-CERT Aviso CiberCOVID19 nueva sec...	01/04/2020 0:04	Elemento de Outl...
 Informe_del_Archivo_document (1).pdf_(28f28eea...	04/04/2020 21:02	Adobe Acrobat D...

La hora más oscura

Pruebas



Mery_pc



CSIRT-CV

Centre Seguretat TIC
de la Comunitat Valenciana

Nuestros compañeros de CsirtCV
prepararon un PC INFERNAL

La hora más oscura

Pruebas


 EPDR
 ESTADO EQUIPOS CONFIGURACIÓN **TAREAS**


 grimaltos_ant
CONSELLERIA DE SANITAT - G...

[< Atrás](#)

Resultados de tarea
 Analizar Mery-PC (16/04/2020 9:08:22)
 [Ver tarea](#)

Análisis lanzado el 16/04/2020 9:08:20
 

Filtros
 

[Ver detecciones \(56\)](#)

Equipo	Grupo	Detecciones	Estado	Fecha de comienzo	Fecha de fin
 Mery-PC	 ExternosSanidad	56	Finalizada	16/04/2020 9:08:58	16/04/2020 9:33:26

La hora más oscura

Pruebas

[Atrás](#)

Analizar Mery-PC (16/04/2020 9:08:22): Detecciones

Ejecución:16/04/2020 9:08:20

Equipo	Grupo	Tipo de amenaza	Ruta	Acción	Fecha
Mery-PC	ExternosSanidad	Virus	C:\Users\Mery\Desktop\Loader_v2_11cr122.exe	Movido a Cuarentena	16/04/2020 9:29:55
Mery-PC	ExternosSanidad	Virus	C:\Users\Mery\chocolatey\chocolatey\chocolatey\kali_windowsbinaries.flare\20190314.1.0.7\kali-windows-binaries-master.zip[kali-windows-binaries-master\klogger.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Virus	C:\Users\Mery\chocolatey\chocolatey\chocolatey\kali_windowsbinaries.flare\20190314.1.0.7\kali-windows-binaries-master.zip[kali-windows-binaries-master\fgdump\servpw64.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Herramientas de hacking y PUPS	C:\Users\Mery\chocolatey\chocolatey\chocolatey\scdbg.flare\20191104.0\scdbg.zip[scdbg.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Herramientas de hacking y PUPS	C:\Users\Mery\chocolatey\chocolatey\chocolatey\kali_windowsbinaries.flare\20190314.1.0.7\kali-windows-binaries-master.zip[kali-windows-binaries-master\fgdump\fgdump.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Herramientas de hacking y PUPS	C:\Users\Mery\chocolatey\chocolatey\chocolatey\kali_windowsbinaries.flare\20190314.1.0.7\kali-windows-binaries-master.zip[kali-windows-binaries-master\fgdump\cachedump.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Herramientas de hacking y PUPS	C:\Users\Mery\chocolatey\chocolatey\chocolatey\kali_windowsbinaries.flare\20190314.1.0.7\kali-windows-binaries-master.zip[kali-windows-binaries-master\fgdump\pstgdump.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Virus	C:\Users\Mery\chocolatey\chocolatey\chocolatey\kali_windowsbinaries.flare\20190314.1.0.7\kali-windows-binaries-master.zip[kali-windows-binaries-master\sbd.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Virus	C:\Users\Mery\chocolatey\chocolatey\chocolatey\kali_windowsbinaries.flare\20190314.1.0.7\kali-windows-binaries-master.zip[kali-windows-binaries-master\fgdump\cachedump64.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Virus	C:\Users\Mery\chocolatey\chocolatey\offcemalscanner.flare\0.5.20180131.5\offcemalscannerinstall.zip[DisView.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Herramientas de hacking y PUPS	C:\Users\Mery\chocolatey\chocolatey\chocolatey\kali_windowsbinaries.flare\20190314.1.0.7\kali-windows-binaries-master.zip[kali-windows-binaries-master\fgdump\fgexec.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Virus	C:\Users\Mery\chocolatey\chocolatey\chocolatey\kali_windowsbinaries.flare\20190314.1.0.7\kali-windows-binaries-master.zip[kali-windows-binaries-master\fgdump\PwDump.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Herramientas de hacking y PUPS	C:\Users\Mery\chocolatey\chocolatey\chocolatey\kali_windowsbinaries.flare\20190314.1.0.7\kali-windows-binaries-master.zip[kali-windows-binaries-master\fgdump\servpw.exe]	Movido a Cuarentena	16/04/2020 9:29:54
Mery-PC	ExternosSanidad	Virus	C:\Users\Mery\AppData\Local\Temp\chocolatey\pmalabs.flare\0.0.1.4\PracticalMalwareAnalysis-Labs.exe	Movido a Cuarentena	16/04/2020 9:26:26
Mery-PC	ExternosSanidad	Herramientas de hacking y PUPS	C:\Users\Mery\AppData\Local\Temp\chocolatey\chocolatey\processhacker.install\2.39\processhacker-2.39-setup.exe	Movido a Cuarentena	16/04/2020 9:23:21
Mery-PC	ExternosSanidad	Virus	C:\Users\Mery\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\71HJCNZX\regasm[1].exe	Movido a Cuarentena	16/04/2020 9:23:19
Mery-PC	ExternosSanidad	Virus	C:\ProgramData\chocolatey\lib\pmalabs.flare\tools\Practical Malware Analysis Labs\BinaryCollection\Chapter_14L\Lab14-01.exe	Movido a Cuarentena	16/04/2020 9:19:34
Mery-PC	ExternosSanidad	Virus	C:\ProgramData\chocolatey\lib\offcemalscanner.flare\tools\DisView.exe	Movido a Cuarentena	16/04/2020 9:19:33
Mery-PC	ExternosSanidad	Virus	C:\ProgramData\chocolatey\lib\offcemalscanner.flare\tools\OfficeMalScanner.zip[DisView.exe]	Movido a Cuarentena	16/04/2020 9:19:33
Mery-PC	ExternosSanidad	Virus	C:\ProgramData\chocolatey\lib\offcemalscanner.flare\offcemalscanner.flare.nupkg[tools\OfficeMalScanner.zip][DisView.exe]	Movido a Cuarentena	16/04/2020 9:19:32
Mery-PC	ExternosSanidad	Virus	C:\ProgramData\chocolatey\lib\kali_windowsbinaries.flare\tools\windows-binaries\kali-windows-binaries-master\sbd.exe	Movido a Cuarentena	16/04/2020 9:18:54
Mery-PC	ExternosSanidad	Virus	C:\ProgramData\chocolatey\lib\kali_windowsbinaries.flare\tools\windows-binaries\kali-windows-binaries-master\klogger.exe	Movido a Cuarentena	16/04/2020 9:18:53
Mery-PC	ExternosSanidad	Virus	C:\ProgramData\chocolatey\lib\kali_windowsbinaries.flare\tools\windows-binaries\kali-windows-binaries-master\fgdump\servpw64.exe	Movido a Cuarentena	16/04/2020 9:18:52
Mery-PC	ExternosSanidad	Herramientas de hacking y PUPS	C:\ProgramData\chocolatey\lib\kali_windowsbinaries.flare\tools\windows-binaries\kali-windows-binaries-master\fgdump\servpw.exe	Movido a Cuarentena	16/04/2020 9:18:50
Mery-PC	ExternosSanidad	Virus	C:\ProgramData\chocolatey\lib\kali_windowsbinaries.flare\tools\windows-binaries\kali-windows-binaries-master\fgdump\PwDump.exe	Movido a Cuarentena	16/04/2020 9:18:49

La hora más oscura

Pruebas

[Atrás](#)

Analizar Mery-PC (16/04/2020 9:08:22): Detecciones

Ejecución:16/04/2020 9:08:20

Equipo	Grupo	Tipo de amenaza	Ruta	Acción	Fecha
☐ Mery-PC	☐ ExternosSanidad	Herramientas de hacking y PUPs	C:\ProgramData\chocolatey\lib\kali_windowsbinaries.flare\tools\windows-binaries\kali-windows-binaries-master\fgdump\pstgdump.exe	Movido a Cuarentena	16/04/2020 9:18:48
☐ Mery-PC	☐ ExternosSanidad	Herramientas de hacking y PUPs	C:\ProgramData\chocolatey\lib\kali_windowsbinaries.flare\tools\windows-binaries\kali-windows-binaries-master\fgdump\fgexec.exe	Movido a Cuarentena	16/04/2020 9:18:47
☐ Mery-PC	☐ ExternosSanidad	Herramientas de hacking y PUPs	C:\ProgramData\chocolatey\lib\kali_windowsbinaries.flare\tools\windows-binaries\kali-windows-binaries-master\fgdump\fgdump.exe	Movido a Cuarentena	16/04/2020 9:18:46
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\lib\kali_windowsbinaries.flare\tools\windows-binaries\kali-windows-binaries-master\fgdump\cachedump64.exe	Movido a Cuarentena	16/04/2020 9:18:45
☐ Mery-PC	☐ ExternosSanidad	Herramientas de hacking y PUPs	C:\ProgramData\chocolatey\lib\kali_windowsbinaries.flare\tools\windows-binaries\kali-windows-binaries-master\fgdump\cachedump.exe	Movido a Cuarentena	16/04/2020 9:18:44
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\whoami.exe	Movido a Cuarentena	16/04/2020 9:18:43
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\unshar.exe	Movido a Cuarentena	16/04/2020 9:18:42
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\recode.exe	Movido a Cuarentena	16/04/2020 9:18:41
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\printf.exe	Movido a Cuarentena	16/04/2020 9:16:10
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\OfficeMalScanner.exe	Movido a Cuarentena	16/04/2020 9:16:10
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\ncat.exe	Movido a Cuarentena	16/04/2020 9:16:09
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\mkfifo.exe	Movido a Cuarentena	16/04/2020 9:16:08
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\MetaPuck.exe	Movido a Cuarentena	16/04/2020 9:16:07
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\md5sum.exe	Movido a Cuarentena	16/04/2020 9:16:06
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\jwhois.exe	Movido a Cuarentena	16/04/2020 9:16:05
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\jd-gui.exe	Movido a Cuarentena	16/04/2020 9:16:04
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\indent.exe	Movido a Cuarentena	16/04/2020 9:16:03
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\hashcalc.exe	Movido a Cuarentena	16/04/2020 9:16:02
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\gunzip.exe	Movido a Cuarentena	16/04/2020 9:16:01
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\fsplit.exe	Movido a Cuarentena	16/04/2020 9:16:00
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\expand.exe	Movido a Cuarentena	16/04/2020 9:15:59
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\factor.exe	Movido a Cuarentena	16/04/2020 9:15:59
☐ Mery-PC	☐ ExternosSanidad	Virus	C:\ProgramData\chocolatey\bin\csplit.exe	Movido a Cuarentena	16/04/2020 9:15:58
☐ Mery-PC	☐ ExternosSanidad	Herramientas de hacking y PUPs	C:\Program Files (x86)\scdbg\scdbg.exe	Movido a Cuarentena	16/04/2020 9:15:41
☐ Mery-PC	☐ ExternosSanidad	Herramientas de hacking y PUPs	C:\Program Files\Process Hacker 2\Process Hacker.exe	Movido a Cuarentena	16/04/2020 9:14:02

La hora más oscura

Pruebas

EPDR

ESTADO

EQUIPOS

CONFIGURACIÓN

TAREAS

< Atrás

Analizar Mery-PC (16/04/2020 9:08:22): Detecciones

Ejecución:16/04/2020 9:08:20

Equipo	Grupo	Tipo de amenaza	Ruta
 Mery-PC	 ExternosSanidad	Herramientas de hacking y PUPs	C:\Program Files\Process Hacker 2\ProcessHacker.exe
 Mery-PC	 ExternosSanidad	Herramientas de hacking y PUPs	C:\PDFStreamDumper\mupdf.dll
 Mery-PC	 ExternosSanidad	Herramientas de hacking y PUPs	C:\PDFStreamDumper\iTextFilters.dll
 Mery-PC	 ExternosSanidad	Virus	C:\\$Recycle.Bin\S-1-5-21-3828987058-1146383009-1324517810-1001\SRUB14E0
 Mery-PC	 ExternosSanidad	Virus	C:\\$Recycle.Bin\S-1-5-21-3828987058-1146383009-1324517810-1001\SR00P5Y8.exe
 Mery-PC	 ExternosSanidad	Virus	C:\\$Recycle.Bin\S-1-5-21-3828987058-1146383009-1324517810-1001\SR4SKJGH.exe

La hora más oscura

Datos estadísticos

1.997 máquinas
registradas y comunicantes

1.464 detecciones de Malware
únicas reportadas

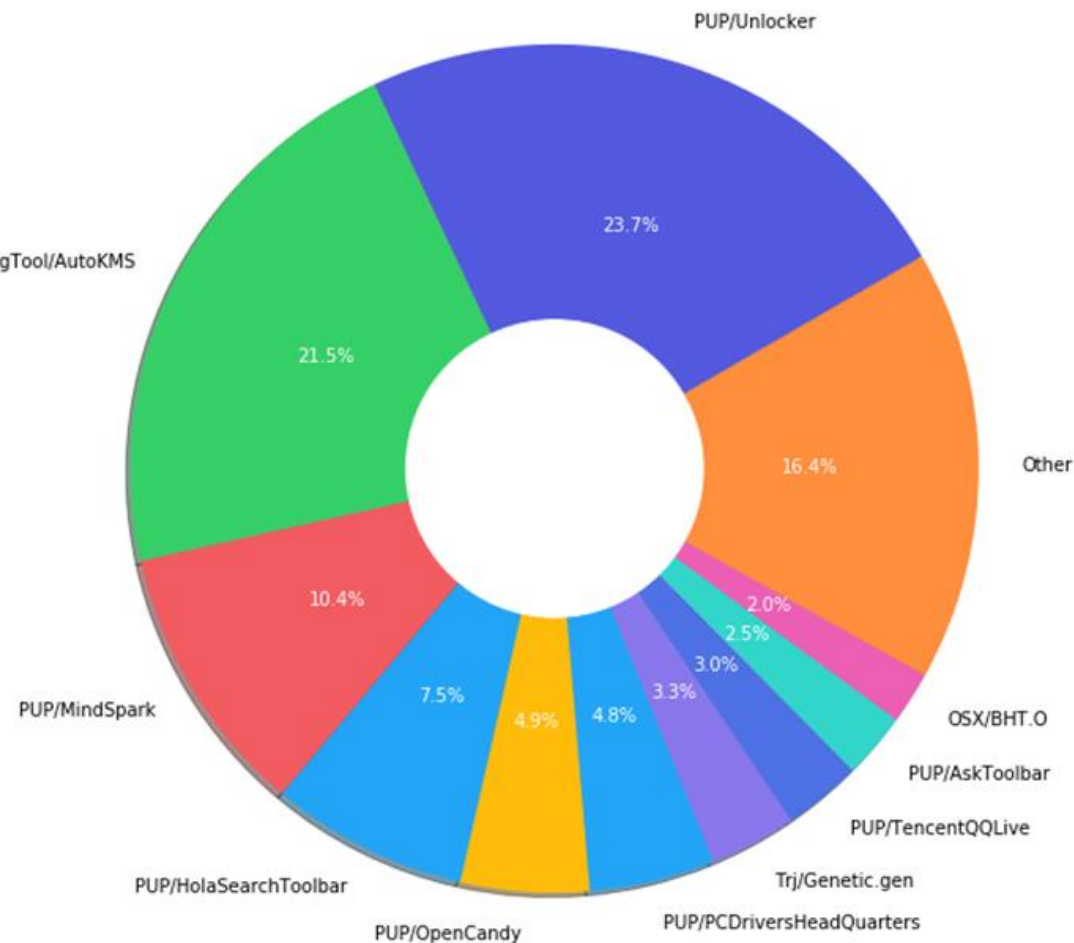
23,39 %
máquinas afectadas con detecciones de Malware

La hora más oscura

1.997 máquinas registradas y comunicantes

1.464 detecciones de Malware únicas reportadas

23,39 % máquinas afectadas con detecciones de Malware



La hora más oscura

PRINCIPAL INCONVENIENTE A LA HORA DE INVESTIGAR INCIDENTES (recibíamos 2 tipos de avisos)

- **DE LA SONDA**, AVISOS CsirtCV, Las direcciones asociadas son las de la VPN, que se asignan dinámicamente:
 - Consulta LOGS CONEXIÓN
- **DE LA CONSOLA CYTOMIC**, Avisos desde la consola de los que solo teníamos el usuario y la ip local:
 - Análisis en profundidad
 - Aislamiento del equipo

Los saltos de línea adicionales de este mensaje se han eliminado.

De: Antonio Grimaltos <grimaltos_ant@gva.es>
Para: [Redacted]
CC: 'Oficina de Seguridad de la Información'; 'CSIRTCV'; [Redacted]
Asunto: RE: URGENTE. RV: [CSIRT-CV #777298] Campaña ransomware NetWalker

Enviado el: miércoles 25/03/2020 14:11

Buenas tardes,

Desde CSIRT-CV le informamos que se está llevando a cabo una campaña de ransomware usando el virus COVID-19 para engañar a los usuarios e infectar sistemas para pedir un rescate.

Os adjuntamos los IOCs que hemos podido recoger hasta el momento para desplegar en el antivirus y evitar que pueda ejecutarse en caso de que algún usuario sea engañado y trate de ejecutar el programa malicioso.

El programa malicioso, en primer lugar, trata de eliminar las copias del sistema guardadas ejecutando un comando del sistema. En caso de tener capacidades de detectar la ejecución de estos programas, notificar en caso de identificar la ejecución del siguiente comando:

`C:\Windows\system32\vssadmin.exe delete shadows /all /quiet`

Hashes SHA256 y SHA1 a bloquear:

00a0f724cf9c3dcde118897a9fd74300faba3ef33aa55b6d5531a606ced45b24
03e5fb84d3de926cba0734000889229bd504f2e8a1143324c5651eaa22d8978
06b8638fdd478672cfe140221233cacfae6d2890446a5c57c8b1317a27d2a036
0aec48e5d0f4fa5f4f4de0564a249d65c399f94f14149f3a19b3d0dc66c64e75
0b62dc536d38af7cedce21f74cb7d6c9ae6378faf9ad8fc6ac1d55c5ba44c0b8
0d0a5a1c0e938f5ff8b017bcd8804b52a00f275890742b8a2622576636c0f2b7
15a4cd4a7baca3961fb0113164434c535af85cedd54744e14a4d4d7b106dd060
1a3a80e5724a3ad68ff4cd11cfb6360a6c1d2f650349dc3148f37ada4de5b530
27c44e526a84740441ccb55994b9a16baef7d6a410a7131c3b5386e3ab4851ee
2a66e29d91a95815eff1e0ed164b916ae3c195e64b32eae59300963fbf3116d9
3ae36b88d84b327f1cc3e7cb92f76d991b5db0776c7161079ef7bcf9e6c6a61b
3f3130d2660e41b6b36a5e98bcd1b2b4e0b7ff017856b15269aa9d60fb414f47
40e1a3fa5f081cc63f88760c50631c27f611bed899e4b46e2c28dd9a78b9b3d5
411c3b13f7935bc7642b8bd7753fdf50f5b00c050c1414b20d6fbf9ebb073611
A16556c9f085ae56e13f32d7c8c99f03efc6974b2897070f46ef5f9736443a8e

Ver más acerca de: grimaltos_ant@gva.es.



La hora más oscura

De: PADThreatHunting

Enviado el: jueves, 28 de mayo de 2020 15:02

Para: grimaltos_ant@gva.es; Adaptive Defense Support <PADSupport@pandasecurity.com>

Asunto: Incidencia 05053762 // Ataque RDP

De: Antonio Grimaltos <grimaltos_ant@gva.es>

Enviado el: viernes 29/05/2020 9:29

Para:

CC:

Asunto: RV: Incidencia 05053762 // Ataque RDP

Bienos días a todos

Esta incidencia la ha enviado el equipo de Threat Hunting (caza de amenazas) de Panda, podría ser grave o no ser nada, pero 58402 intentos de conexión por RDP son muchísimos.

He cambiado al equipo de grupo y he lanzado un análisis en profundidad.

Ahora veremos...

Adaptive Defense Support Team

PADSupport@pandasecurity.com
pandasecurity.com

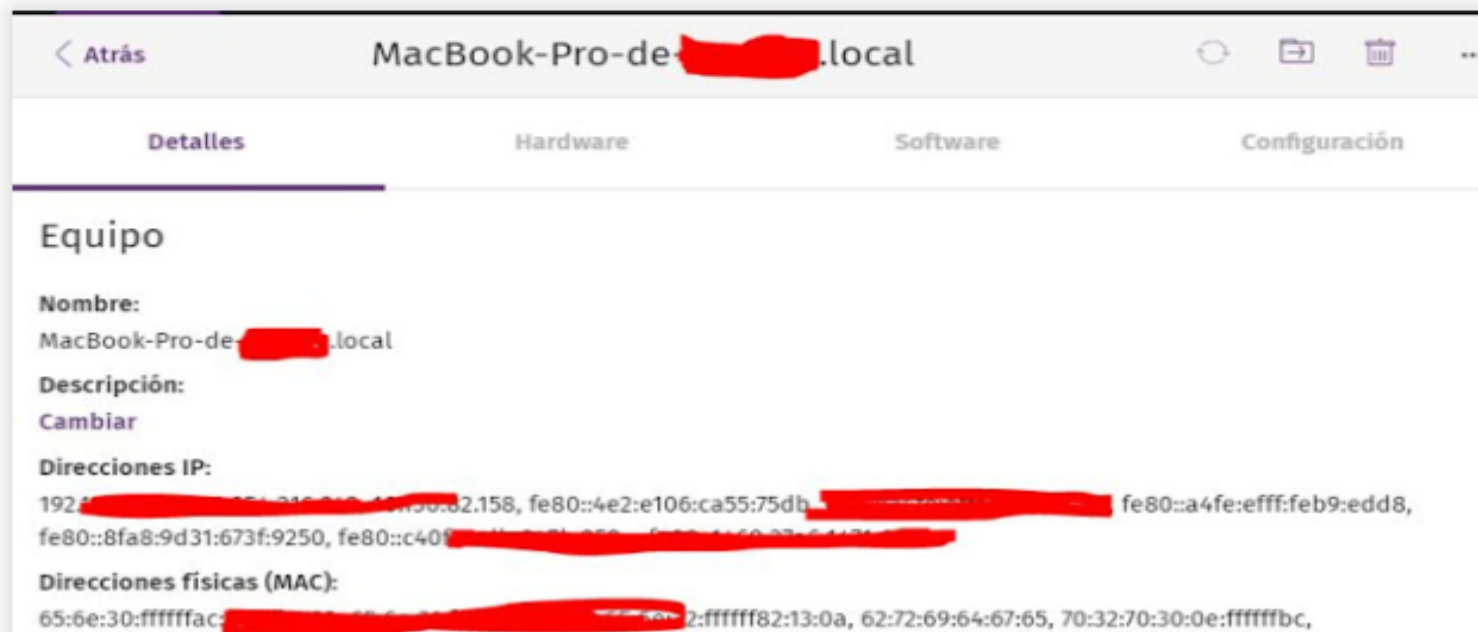
Querido blog,

Existe una leyenda (bueno en realidad dos), que dice que había un usuario que viva en NUNCA JAMÁS, y tenía un Mac, era el rey del Mambo y tocaba canciones de amor. Estaba a salvo siempre (la bruja no estaba en el cuento) porque en un Mac no entran virus...

... Siento estropear el cuento (en realidad no lo siento). Si que hay bruja, y aquí tenemos un usuario con un mac, version del sistema operativo:

macOS Catalina (Version: 10.15) (Build: 19E266)

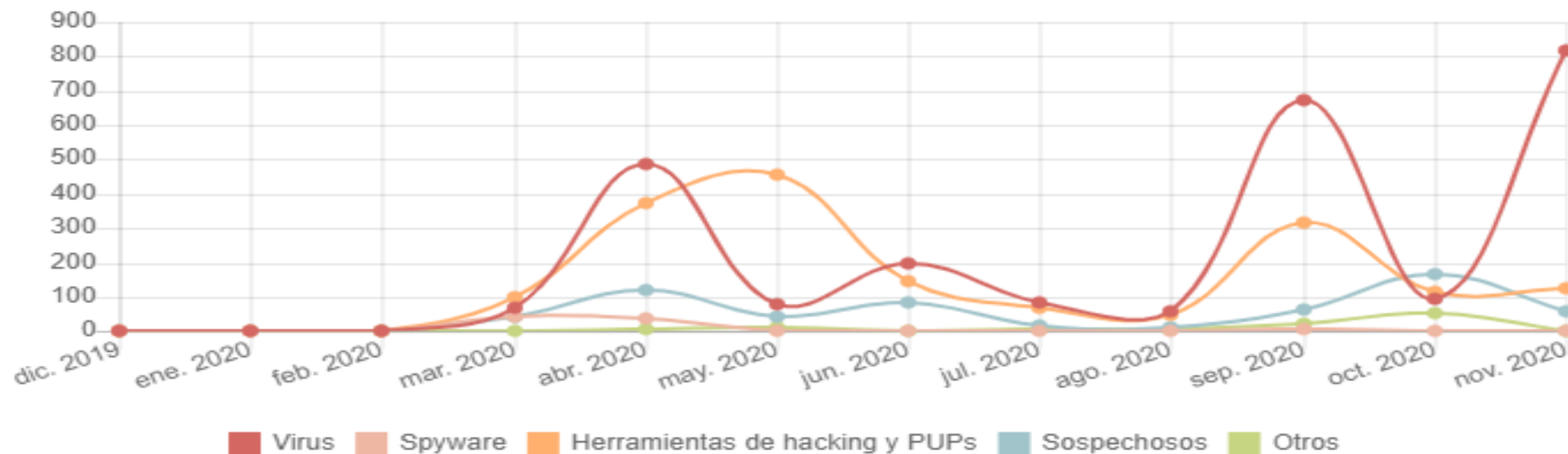
Esta en la foto del equipo:



La hora más oscura

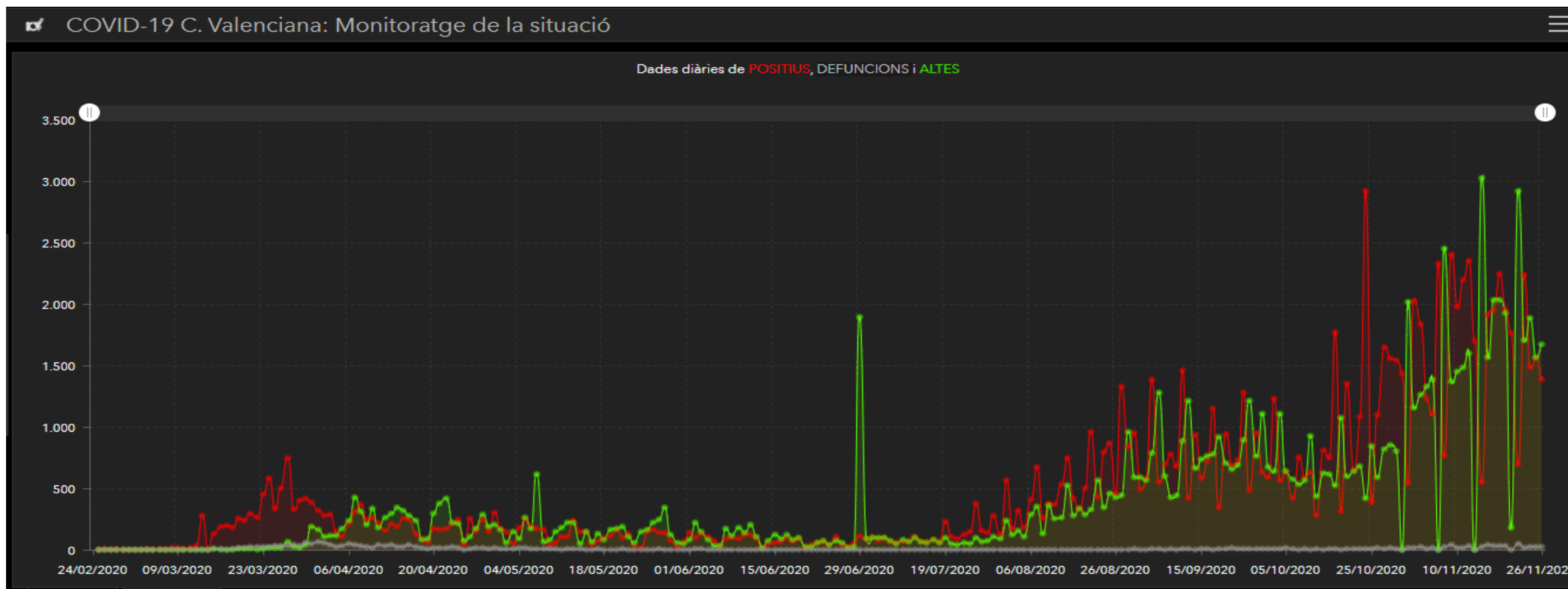
Nuestra consola

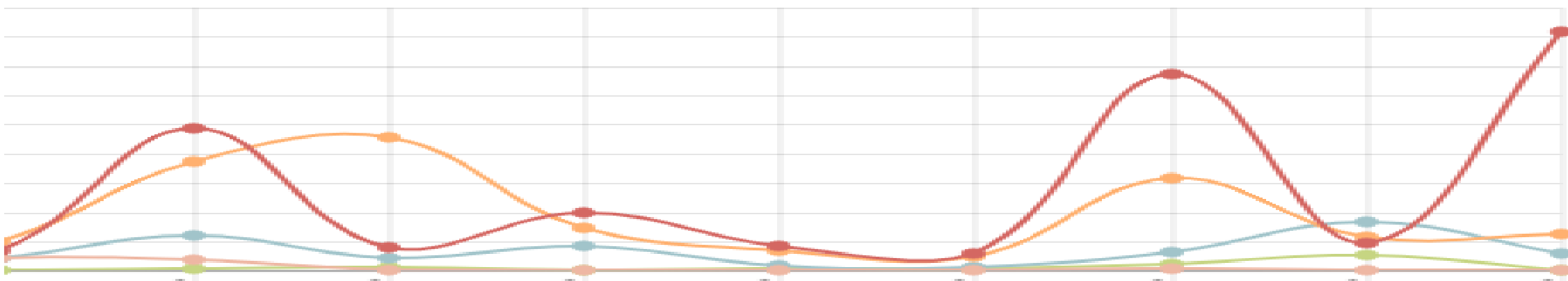
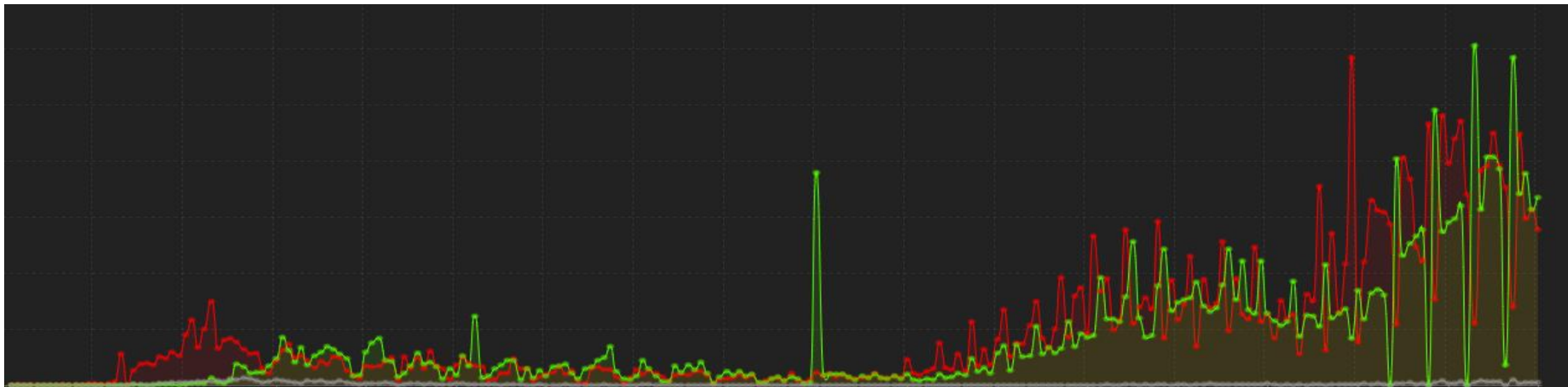
AMENAZAS DETECTADAS POR EL ANTIVIRUS



La hora más oscura

Evolución Covid-19 Comunidad valenciana

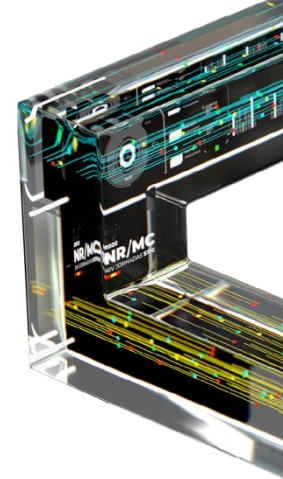
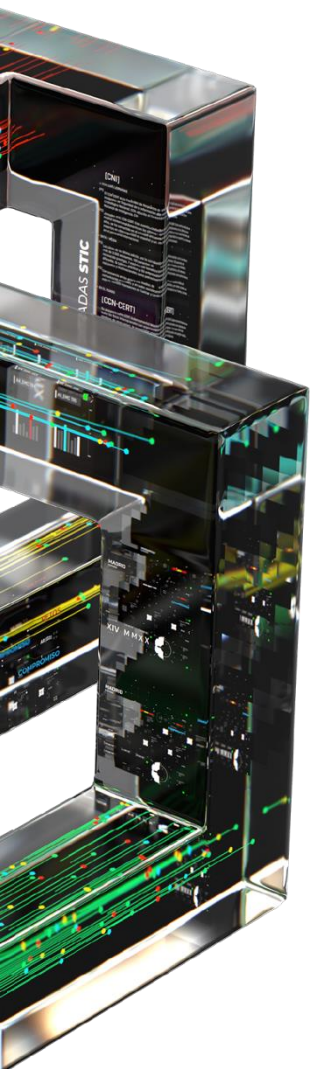




La hora más oscura

AGRADECIMIENTOS

- Cytomic
- Csirt-CV
- Sistemas
- Aplicaciones
- GPT
- CATS
- Y toda la Subdirección General SGSIS
- Arterias
- OSI



MUCHAS GRACIAS

#XIVJORNADASCCNCERT