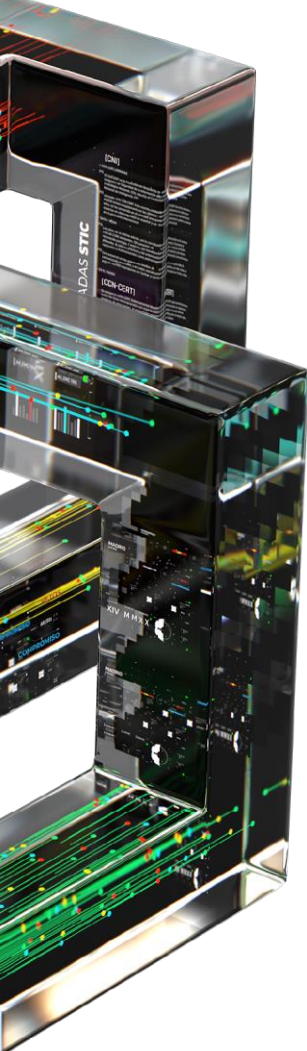




#XIVJORNADASCCNCERT

“Herramientas de conexión remota”



Xavier González

***CTO y Co-Founder
Open Cloud Factory***

xavier.gonzalez@opencloudfactory.com

1. ¿Por qué necesito herramientas?

Tendencias 2020. Tele N

Tele N: El impacto en la administración pública

- Teletrabajo
- Tele docencia
- Tele investigación
- Tele operación / mantenimiento

• La cruda realidad es que durante el confinamiento la administración electrónica y el teletrabajo han sido la única manera de mantener en funcionamiento una parte de los servicios públicos.

Fuente: Teletrabajo y otros retos del Sector Público tras el COVID-19 Thomson Reuters

Archivo JMCadenas EXPANSION

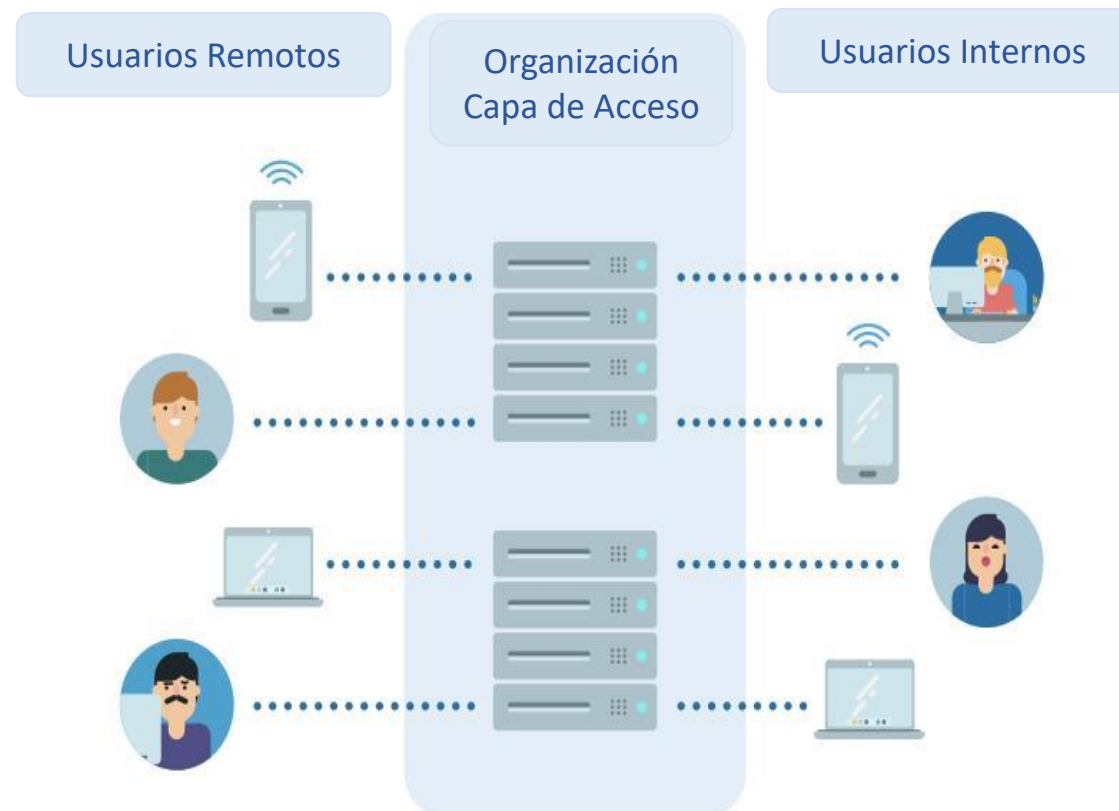
La **regulación del teletrabajo** para en torno a 2,5 millones de empleados públicos de todas las administraciones públicas españolas **entra en vigor hoy**, y las administraciones que deban adaptar su normativa de a lo previsto en el real decreto-ley dispondrán de un plazo de seis meses para hacerlo.

Fuente: Expansión

2. ¿Por qué necesito herramientas?

Seguridad. Zero Trust

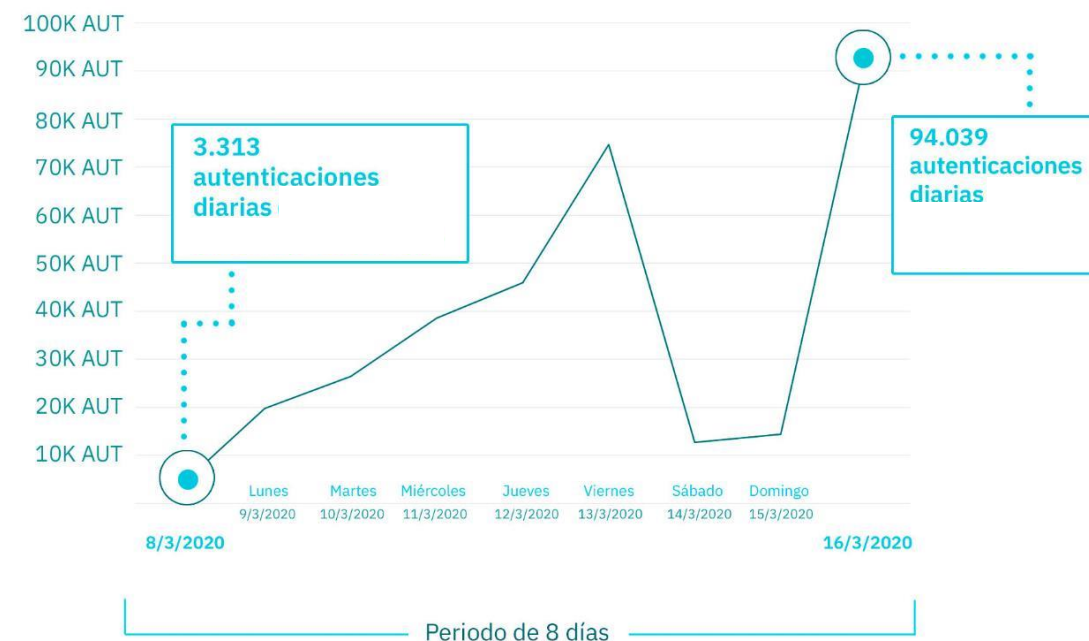
- *Zero Trust* dentro y fuera de la organización
- Fuera supone más riesgo potencial:
 - Dispositivos no corporativos
 - No hay contexto / control / vigilancia de la red "local": la casa ya es parte de la superficie de exposición



3. ¿Por qué necesito herramientas?

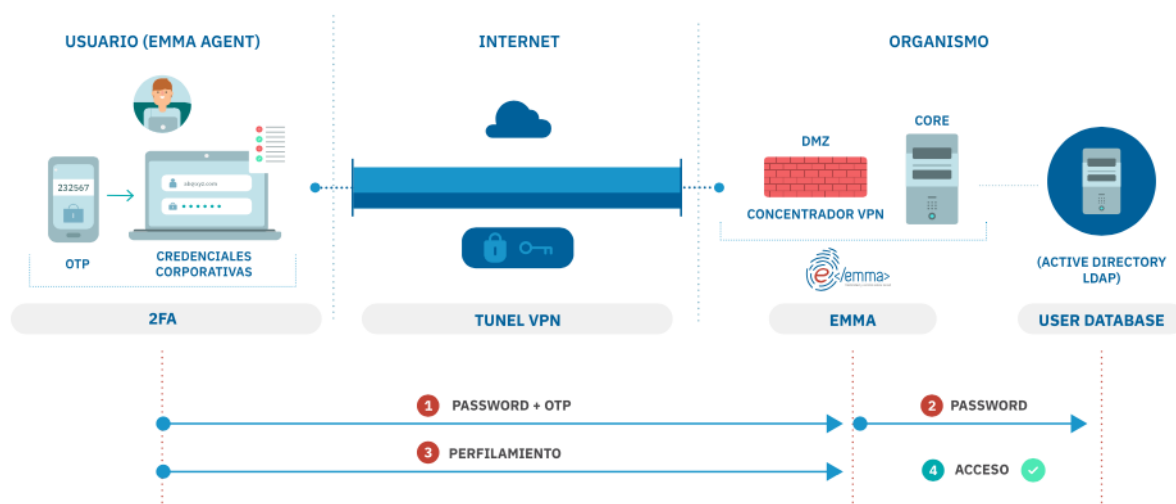
Velocidad del cambio

- De la noche a la mañana
- No permite largos plazos de aprovisionamiento de HW, etc.
- Plan de contingencia
 - El acceso puede variar mucho en función de la necesidad en un momento dado:
 - Semana 21 remotamente
 - Semana 22 desde la oficina



4. EMMA- Vigilancia en accesos remotos

Alto nivel



- Velocidad: Solución de software
 - Lanzada en Abril
 - Aprovecha la infraestructura existente (AD, LDAP)
 - Instalación de agente en equipos remotos
- Seguridad
 - Medidas complementarias de vigilancia
 - Políticas para acceso externo y / o interno (dinámicas)

5. EMMA - Vigilancia en accesos remotos

Seguridad

Perfilado continuo y en tiempo real

- El perfilado del equipo se logra automáticamente en la conexión (SW del equipo y su características) y es continuo, lo que permite averiguar la postura de seguridad del dispositivo

Canal seguro

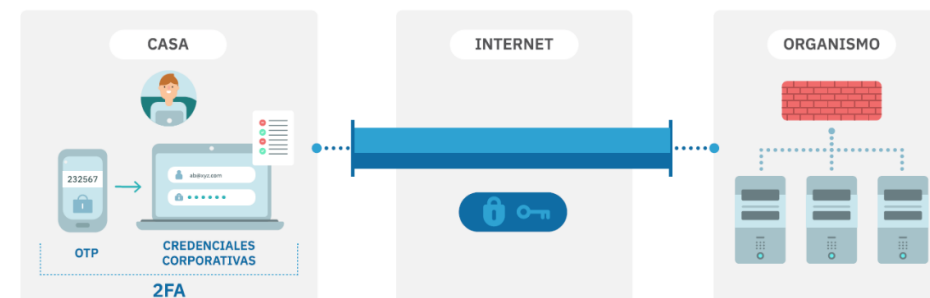
- Comunicación vía un canal cifrado: **Verificación robusta**
- Autenticación del usuario contra LDAP, AD etc. y permite 2FA

Motor de políticas: acceso en función de:

- Permisos de acceso del usuario asociados a su identidad
- Postura de seguridad del equipo
- Horario de la conexión, etc.

Vigilancia entre el usuario y el sistema

- Monitorización del **tráfico** y **comportamiento** entre el usuario y el sistema

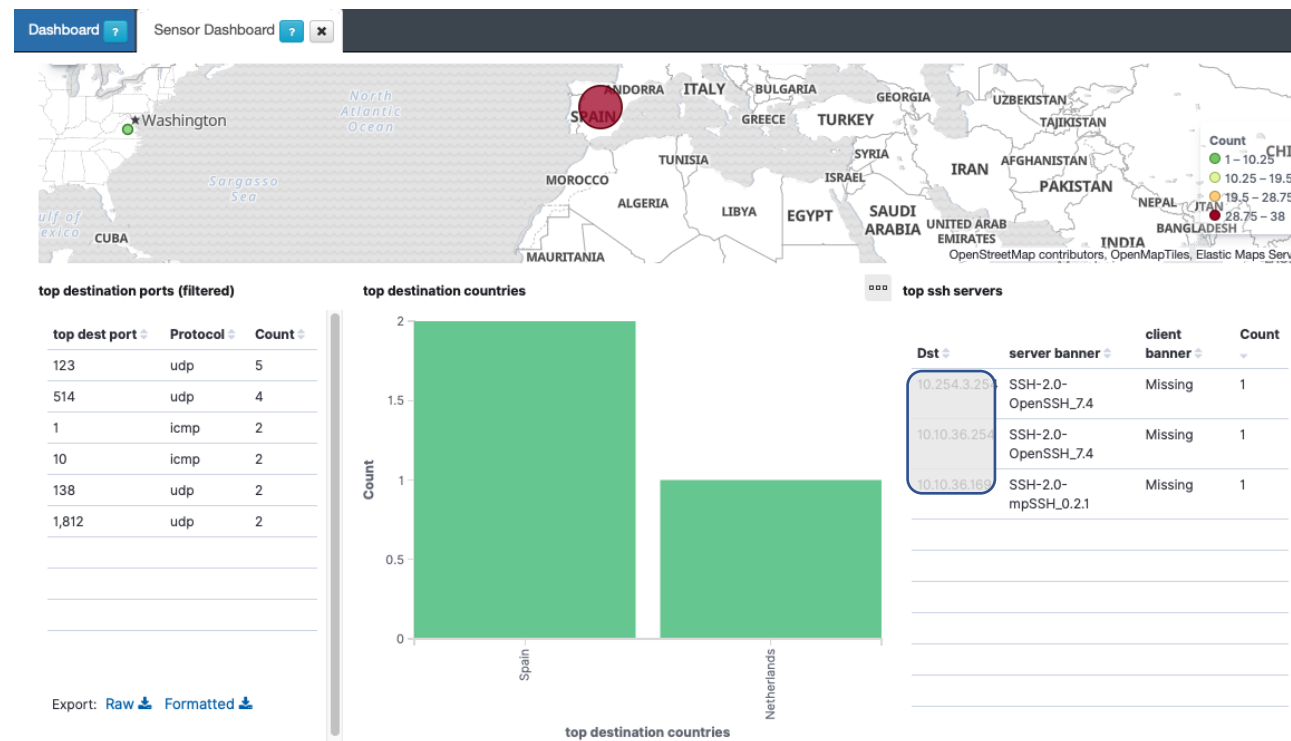


6. EMMA- Vigilancia en accesos remotos

Vigilancia continua del comportamiento

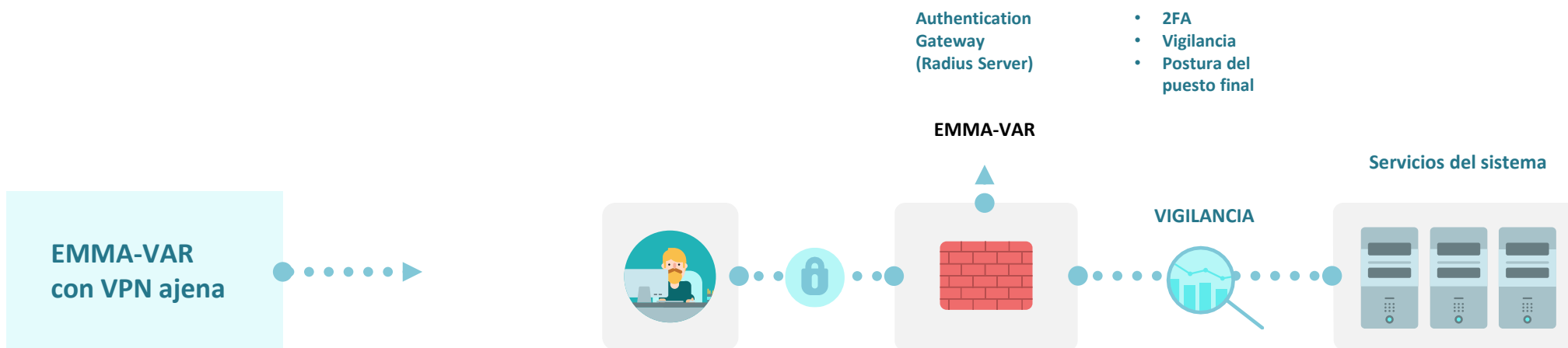
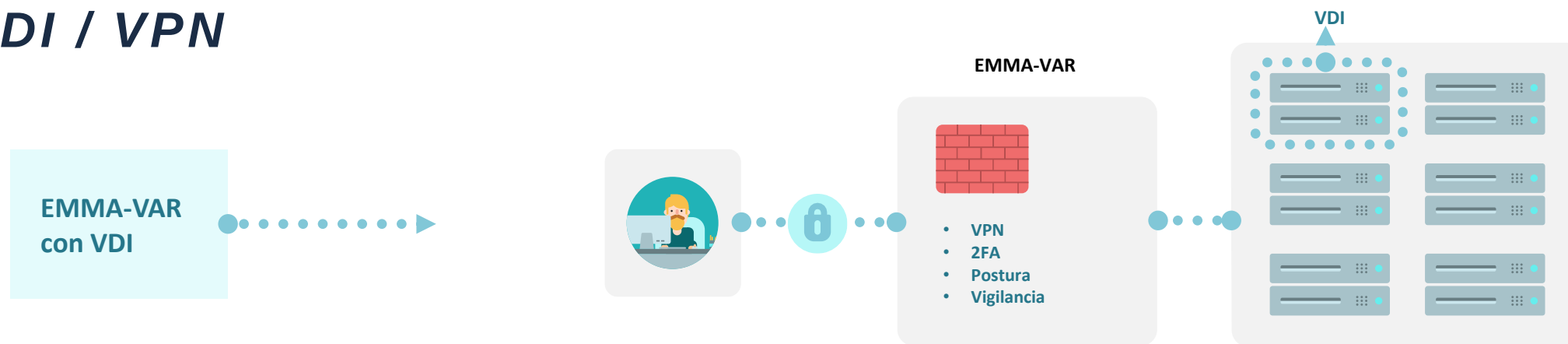
Ejemplos:

- Encontrar usuarios con la contraseña comprometida
- Identificar usuarios con muchas sesiones
- Identificar sesiones con mucho tráfico
- Filtrado por protocolos (RDP etc.)
- Etc.



7. Medidas complementarias

VDI / VPN



8. Gestión centralizada

Valor de la gestión centralizada

- Políticas centralizadas y dinámicas
 - Acceso / permisos a servicios en función de los perfiles / riesgos
 - Hoy desde la oficina
 - Post-condiciones (2FA, postura del equipo, ACLs etc.)
 - Mañana desde cable / wi-fi
 - Post condiciones (ACLs)

General			
Name:	Conexión remota desde equipos corporativos	Enabled:	Yes
Comment:	Conexión remota desde equipos corporativos con LDAP	Created:	2020-11-24 13:59:32
Modified:	2020-11-24 13:59:32		
Preconditions: Time			
Preconditions: Users			
Preconditions: User Devices			
Preconditions: Network Devices			
Preconditions: Sources			

9. Casos de uso EMMA

Organismos que ya han implementado la solución



***Diputación
de León***



***Universidad
de Sevilla***

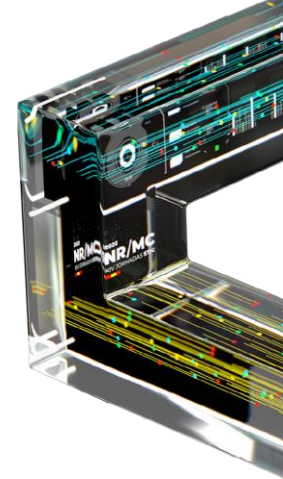
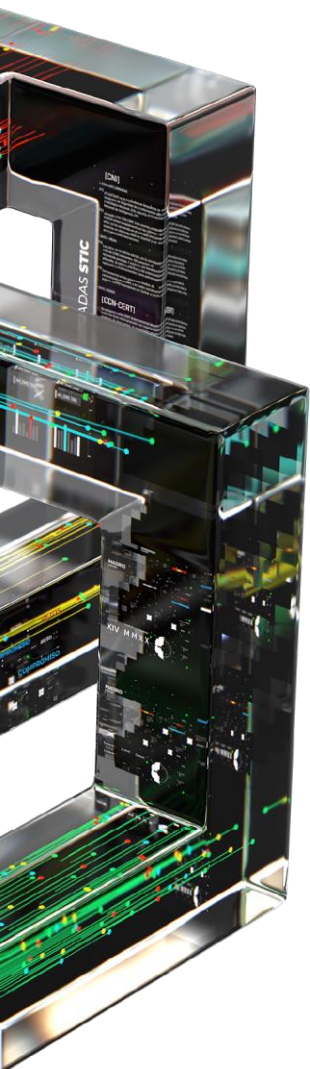


***Ayuntamiento
de Alzira***

*Áreas de pertenencia de
otros organismos que han
implementado EMMA:*

Defensa

***Fuerzas de
seguridad***



MUCHAS

#XIVJORNADASCCNCERT
GRACIAS