Asegurando el acceso privilegiado

Fernando Rubio Román

Microsoft

Secuencia temporal de un ataque típico y observaciones

Sofisticación de ataques

Los atacantes explotan cualquier debilidad

Su objetivo es la información en cualquier dispositivo o servicio

Objetivos: DA & Identidades

El Directorio Activo controla el acceso a los activos del negocio

Los atacantes se enfocan de manera común en el DA y los Administradores de IT

Los ataques no son detectados

Las herramientas actuales de detección no cubren la mayoría de los ataques

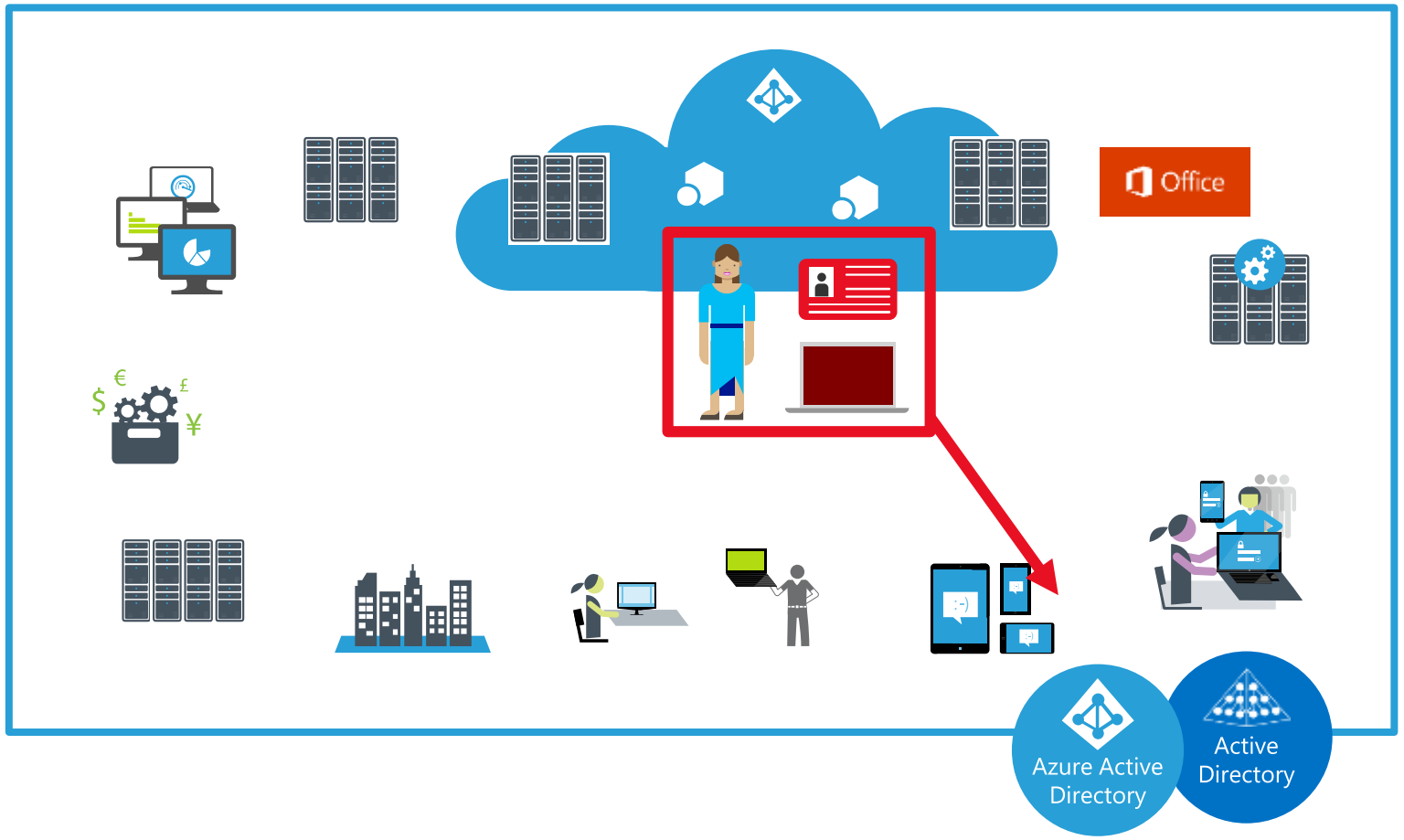
Respuesta y Recuperación

La respuesta requiere concocimientos y herramientas avanzados

Ser capaz de recuperse correctamente a un ataque es caro y difícil de llevar a cabo

La Identidad es el nuevo perímetro de la seguridad

El Directorio Activo y sus administradores controlan todos los activos



Estas prácticas continuan siendo importantes

Parte de una estrategia de seguridad a largo plazo completa

Parches de seguridad de los controladores de Dominio

Objetivo para el despliegue completo 7 días

Eliminar a los usuarios de los administradores locales de los puestos

Objetivo cerca de 0 excepciones

Lineas bases de seguridad

Aplicar configuraciones estandar
Configuración como código (DSC…)

Anti-Malware

Detectar y eliminar amenazas conocidas

Logs de auditoria

Centralizar los logs para el análisis

Inventariado y despliegue de software centralizado

Asegurar la visibilidad y control de los dispositivos para permitir operaciones de seguridad sobre los mismos

Una estrategia completa

Asegurar el acceso privilegiado

Asegurar los activos de alto valor

Seguridad en el datacenter

Protección de la información

Protección de los usuarios y sus dispositivos

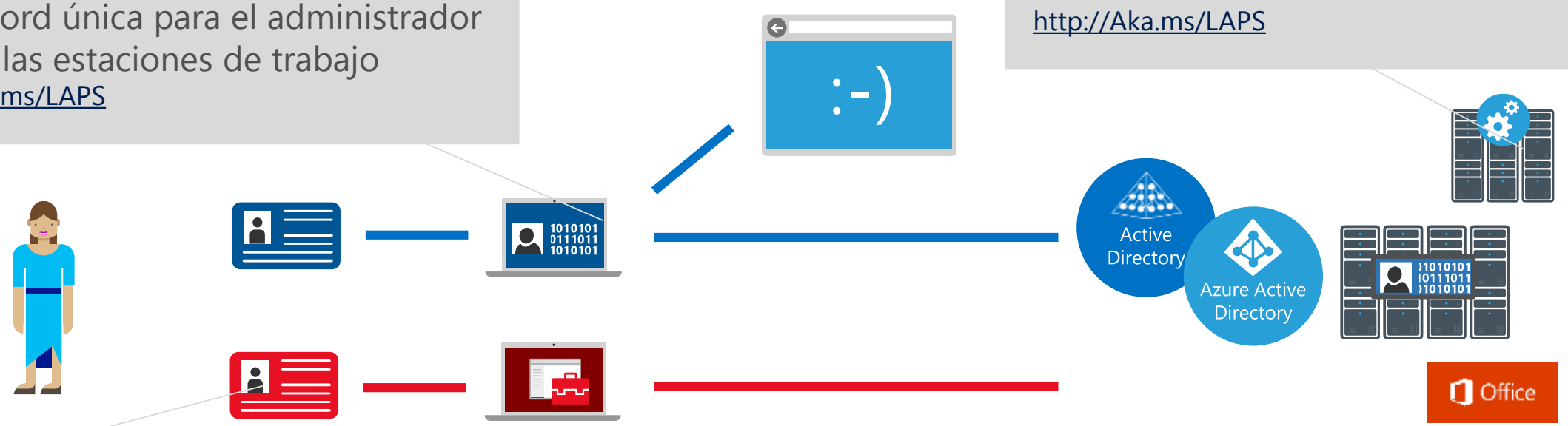
Proteger el Directorio Activo y los privilegios de Administración

2-4 semanas | 1-3 meses | 6+ meses

La primera respuesta para los ataques más comunes

3. Password única para el administrador local de las estaciones de trabajo
http://Aka.ms/LAPS

4. Password única para el administrador local de los servidores
http://Aka.ms/LAPS



1. Cuentas de administración separadas para las tareas de administración

Estaciones de trabajo de acceso privilegiado (PAW)
Fase 1 – Administración de Directorio Activo
http://Aka.ms/CyberPAW

Proteger el Directorio Activo y los privilegios de Administración

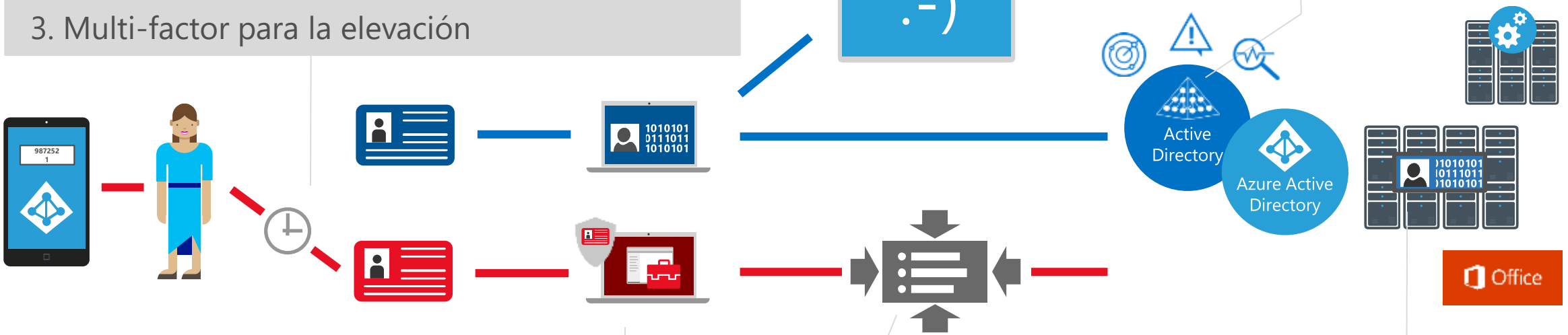
2-4 semanas | 1-3 meses | 6+ meses

Crear visibilidad y control de la actividad de los administradores, incrementar la proteccion frente a ataques típicos

2. Privilegios limitados en el tiempo (JIT)
http://aka.ms/PAM http://aka.ms/AzurePIM

3. Multi-factor para la elevación

6.Detección de ataques
http://aka.ms/ata



1. Estaciones de trabajo de acceso privilegiado (PAW)
Fases 2 y 3, todos los administradores y hardening adicional (Credential Guard, RDP Restricted Admin, etc.)
http://aka.ms/CyberPAW

4. Just Enough Admin (JEA) para la administración de AD
http://aka.ms/JEA

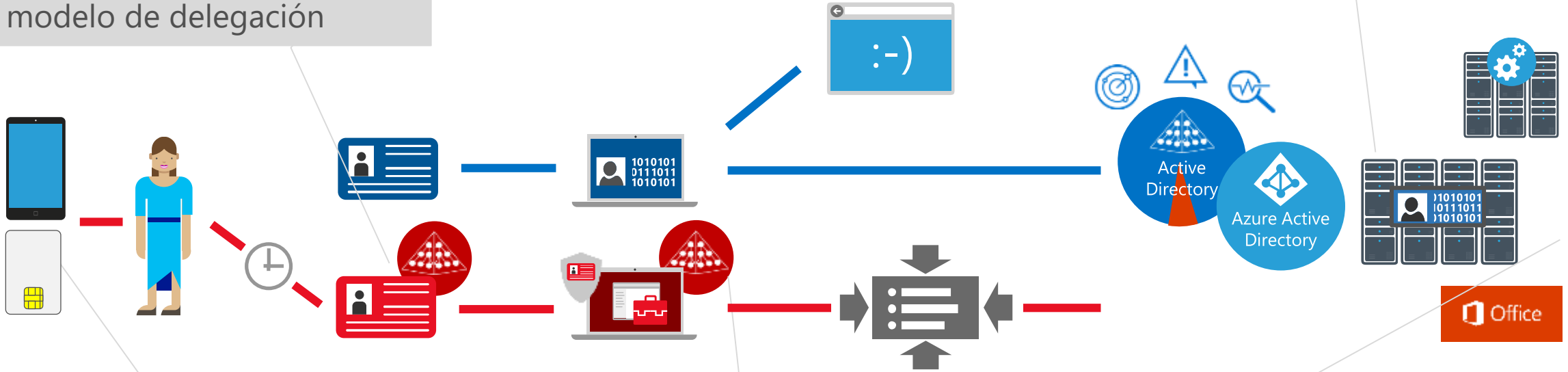
5. Reducir la superficie de ataque del dominio y los DCs
http://aka.ms/HardenAD

Proteger el Directorio Activo y los privilegios de Administración

2-4 semanas | 1-3 meses | 6+ meses

Adoptar una postura proactiva de seguridad

1. Modernizar los roles y el modelo de delegación



5. Shielded VMs para los DCs virtuales (Server 2016 Hyper-V)
http://aka.ms/shieldedvms

2. Autenticación por Smartcard o Passport para todos los administradores
http://aka.ms/Passport

3. Bosque de administración para los administradores y sus estaciones de trabajo
http://aka.ms/ESAE

4. Políticas de integridad de código para los DCs (Windows Server 2016)

© 2016 Microsoft Corporation. All rights reserved. Microsoft, Windows, and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.