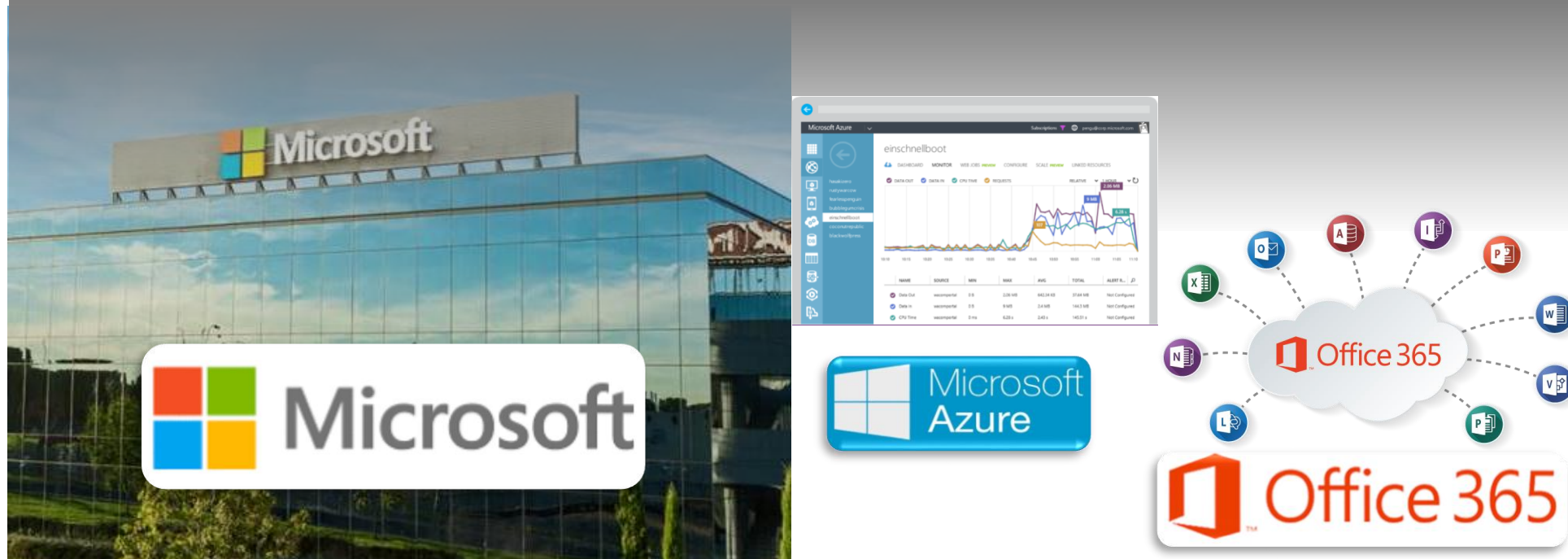


Presentación de la Auditoria de Office 365 y Microsoft Azure frente al Esquema Nacional de Seguridad



MICROSOFT (Microsoft España)
Diciembre de 2015

IX JORNADAS STIC CCN-CERT

ÍNDICE DE CONTENIDOS

- La importancia de Microsoft en la Administración
- Compromiso Microsoft con la Administración
- Objetivo y alcance del proyecto ENS en Microsoft
- Enfoque y Metodología
- Estado Actual
- Factores Clave
- Conclusiones

*What matters to you,
matters to us*

MICROSOFT Y EL ESQUEMA NACIONAL DE SEGURIDAD

La importancia de Microsoft en la Administración

Tal es la relevancia de Microsoft que el Centro Criptológico Nacional ha desarrollado:

- Guías específicas de cumplimiento del ENS (serie “800”) para sistemas Microsoft (CCN-STIC-850A, CCN-STIC-851A, CCN-STIC-859, CCN-STIC-860, CCN-STIC-870A, CCN-STIC-870B, CCN-STIC-850B y CCN-STIC-851B).

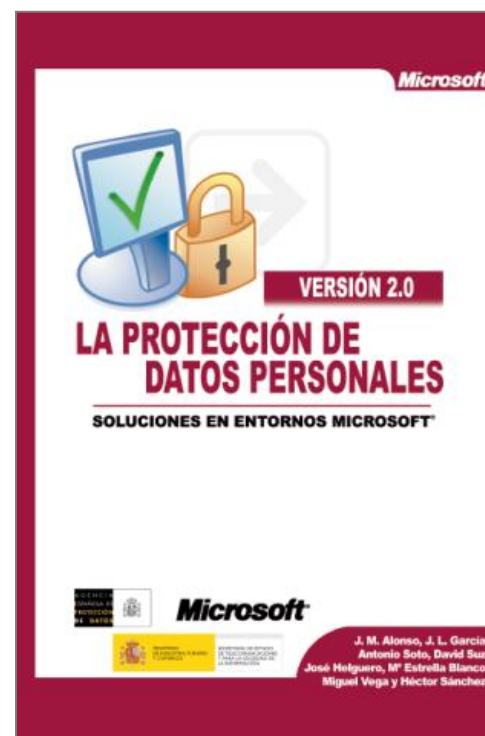


MICROSOFT Y EL ESQUEMA NACIONAL DE SEGURIDAD

Compromiso Microsoft con la Administración

Microsoft, consciente de la importancia del Esquema Nacional de Seguridad colabora con la Administración desarrollando numerosas iniciativas como:

- Compartición del código fuente de sistemas operativos y aplicaciones con el CCN/CNI.
- La publicación del Manual de cumplimiento del Reglamento del ENS y LOPD con tecnología Microsoft.
- La resolución de declaración de adecuación para las transferencias internacionales de datos en la nube.



MICROSOFT Y EL ESQUEMA NACIONAL DE SEGURIDAD

Objetivo y alcance del proyecto ENS en Microsoft

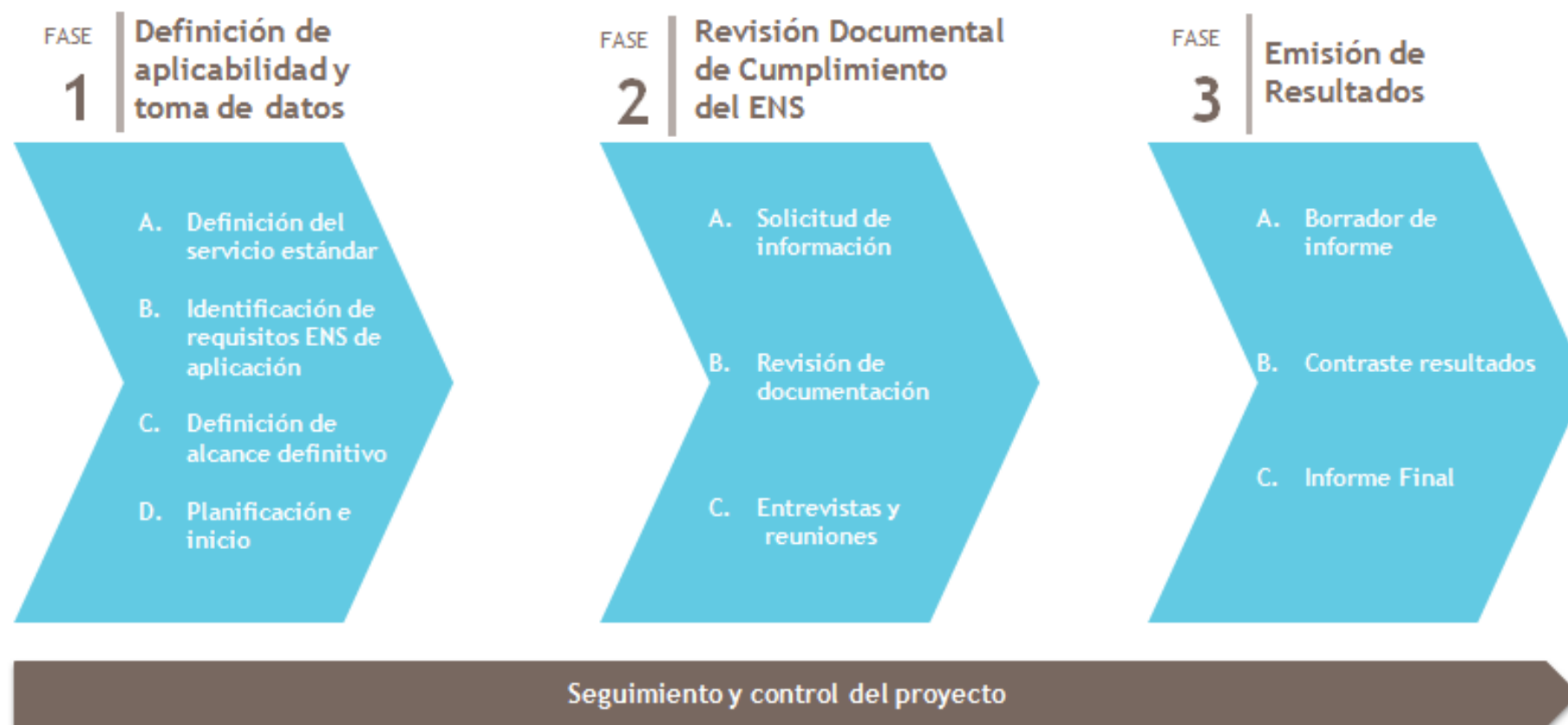


- 1 Microsoft, con el propósito de posicionarse como un proveedor de referencia en el cumplimiento del ENS ha iniciado un proyecto de revisión de sus servicios.
- 2 De esta manera, Microsoft quiere presentarse como un modelo de transparencia, siendo un proveedor que aplica las exigencias de auditoría del ENS para las administraciones públicas.
- 3 Para ello ha contratado los servicios de la BDO, Firma independiente reconocida por sus trabajos de auditoría en el Esquema Nacional de Seguridad.
- 4 Este proyecto cuenta tanto con el apoyo y soporte de los responsables nacionales e internacionales de Microsoft.
- 5 El enfoque de la revisión consistirá en una evaluación en dos fases:
Fase 1: Evaluación documental previa con el fin de revisar aspectos procedimentales.
Fase 2: Evaluación operativa para revisar que la operativa del servicio es conforme al ENS.

MICROSOFT Y EL ESQUEMA NACIONAL DE SEGURIDAD

Enfoque y Metodología

A continuación se presenta el enfoque metodológico, utilizado para cubrir los objetivos y el alcance determinados para el presente Proyecto de la revisión documental de cumplimiento del ENS:



MICROSOFT Y EL ESQUEMA NACIONAL DE SEGURIDAD

Estado Actual

- 1 Actualmente se ha realizado la revisión documental del servicio O365 y se dispone de un estado avanzado de la revisión del servicio AZURE.
- 2 Microsoft ha desarrollado los documentos “System Security Plan” (SSP) específicos para los diferentes servicios:
 - Microsoft Office 365
 - AZURE
- 3 Los SSP presentan el alineamiento del marco de control de la seguridad de cada servicio con el Esquema Nacional de Seguridad.
- 4 Partiendo de estos documentos se procede a la solicitud de información adicional complementaria en aquellos requisitos en los que se requiera un detalle adicional.
- 5 Como resultado de la revisión se ha concluido que a nivel documental no se han identificado aspectos de incumplimiento.

MICROSOFT Y EL ESQUEMA NACIONAL DE SEGURIDAD

Factores Clave

- 1 Enfoque del Esquema Nacional de Seguridad como una necesidad regulatoria y una oportunidad de incrementar la seguridad.
- 2 Apoyo de responsables de Microsoft:
 - A nivel local
“Chief Technology Officer”, “Enterprise Strategy Consultant”, “Corporate, External & legal Affairs”, “Microsoft Corporation Office 365 Business Group”, “Solutions Technology Unit”.
 - A nivel internacional
“Senior Program Manager” e “International Regulatory Compliance”.
- 3 Conocimiento de la operativa, estructura y responsables a nivel nacional e internacional.
- 4 Conocimiento de los servicios concretos ofertados al cliente.

MICROSOFT Y EL ESQUEMA NACIONAL DE SEGURIDAD

Conclusiones

- 1 Se ha identificado que requisitos del ENS son de aplicación a los servicios de Microsoft.
- 2 Se han identificado los controles internos de la Compañía que permiten cumplir con el ENS.
- 3 Se han identificado las configuraciones específicas a establecer cuando se ofrecen servicios a la Administración.
- 4 Se ha aportado visibilidad a las áreas internacionales de Microsoft de las exigencias regulatorias españolas y los controles necesarios para su cumplimiento.
- 5 Se ha conseguido la implicación de equipos internacionales de Microsoft en las tareas de cumplimiento del ENS.

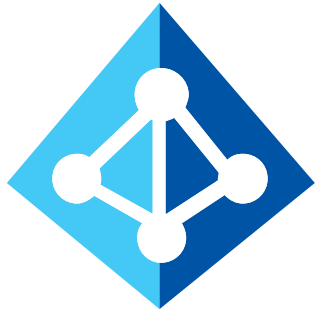
Muchas Gracias

valentin.faura@bdo.es

Gestión de Identidades

Microsoft Azure Active Directory

¿Que es Microsoft AAD?

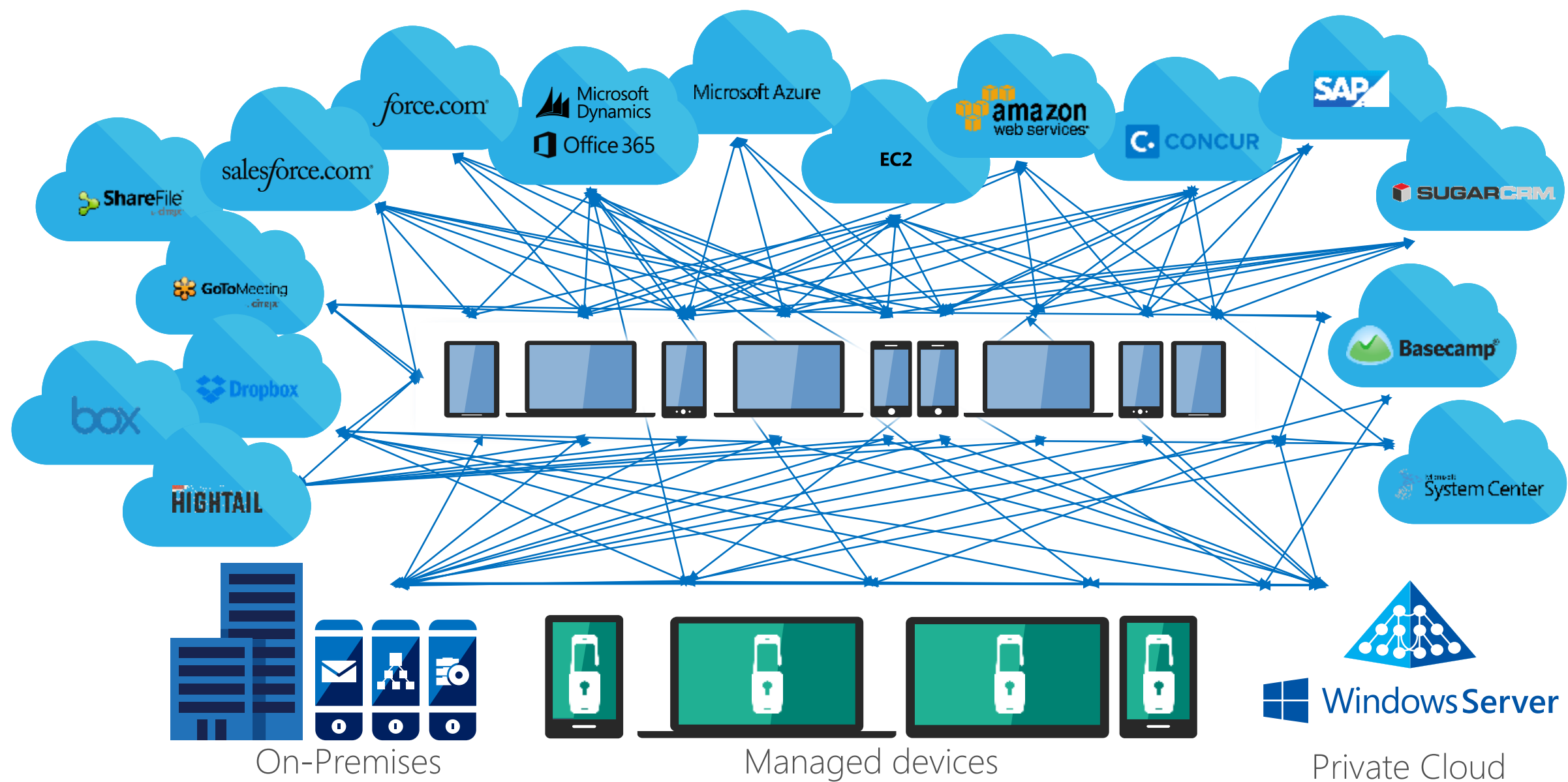


B2E B2B B2C

Una solución de identidad y acceso para empleados, partners y clientes.

Combina servicios de directorio, **gobernanza de la identidad y gestión de acceso** a las aplicaciones y plataforma basada en **estándares** para desarrolladores.

Un mundo repleto de dispositivos y aplicaciones SaaS



Acceso Seguro a cualquier aplicación desde cualquier sitio

Aplicaciones en/de nube



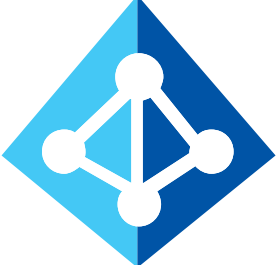
Aplicaciones locales de la organización

Proveedores de Identidad



acceso

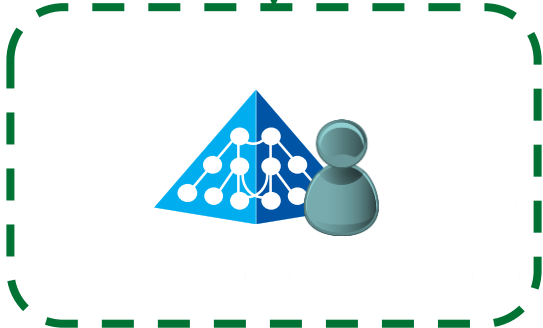
acceso



acceso

Acceso condicional

- ✓ Localización
- ✓ Estado del dispositivo
- ✓ Pertenencia a grupo



Plataforma de Federación de mi organización

- ▶ Single Sign On
- ▶ Segundo factor de autenticación
- ▶ Informes y auditoria
- ▶ Autoservicio



"Azure Active Directory B2C helps us bring the stadium closer to our 450 million fans around the globe with simplified registration and login through social accounts like Facebook, or traditional username/passwords login."

RAFAEL DE LOS SANTOS

HEAD OF DIGITAL
REAL MADRID

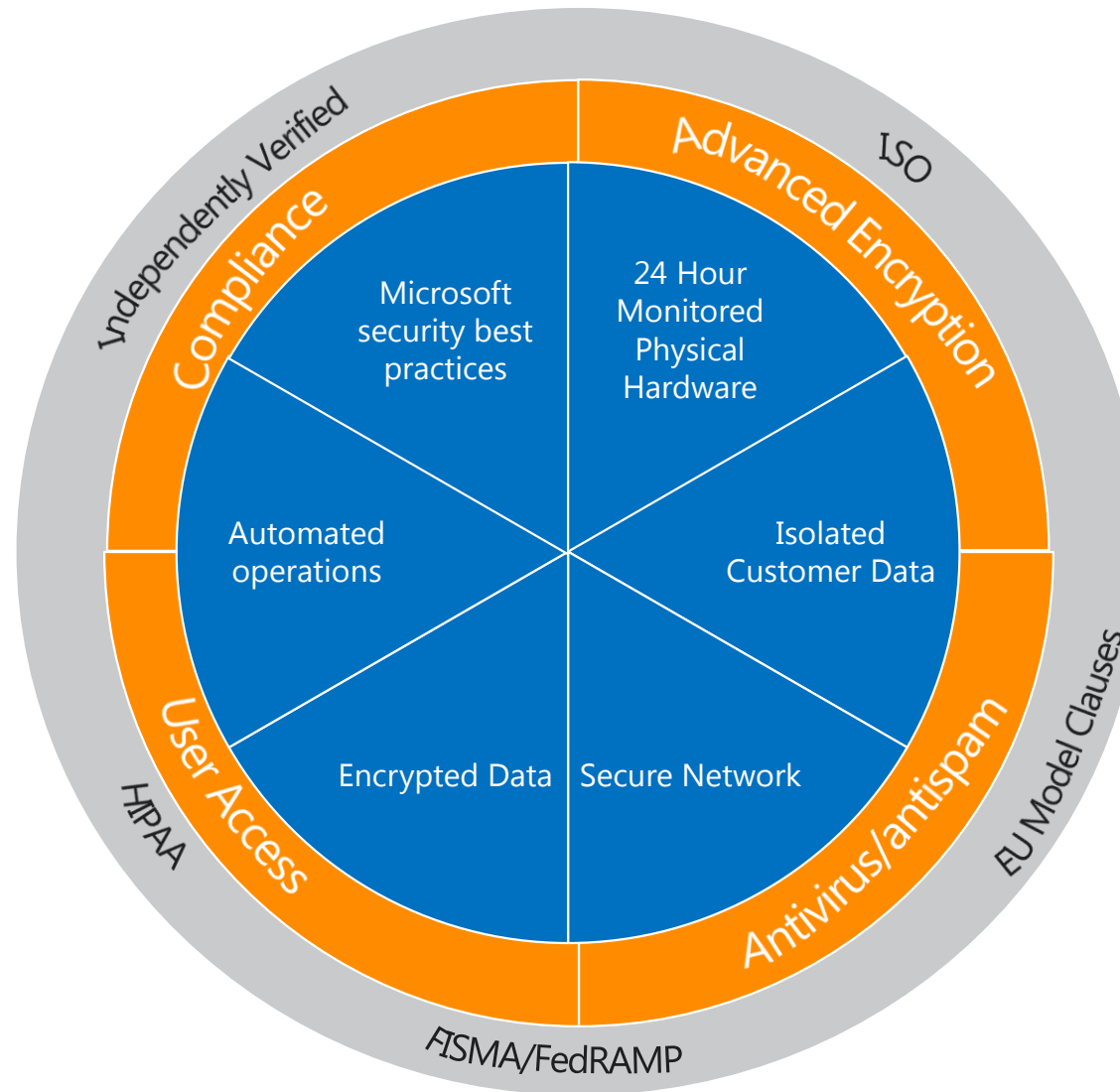
- Provided a seamless experience across mobile applications on any platform
- Built a fully customized login page without custom code
- Alleviated concerns about security, data breaches, and scalability

Seguridad con Office 365



Seguridad con Office 365

- Seguridad Office 365
- Controles cliente
- Auditorías externas



Cifrado avanzado



Cifrado avanzado



Cifrado en almacenamiento



Azure
containers



Gestión de las claves por parte del cliente



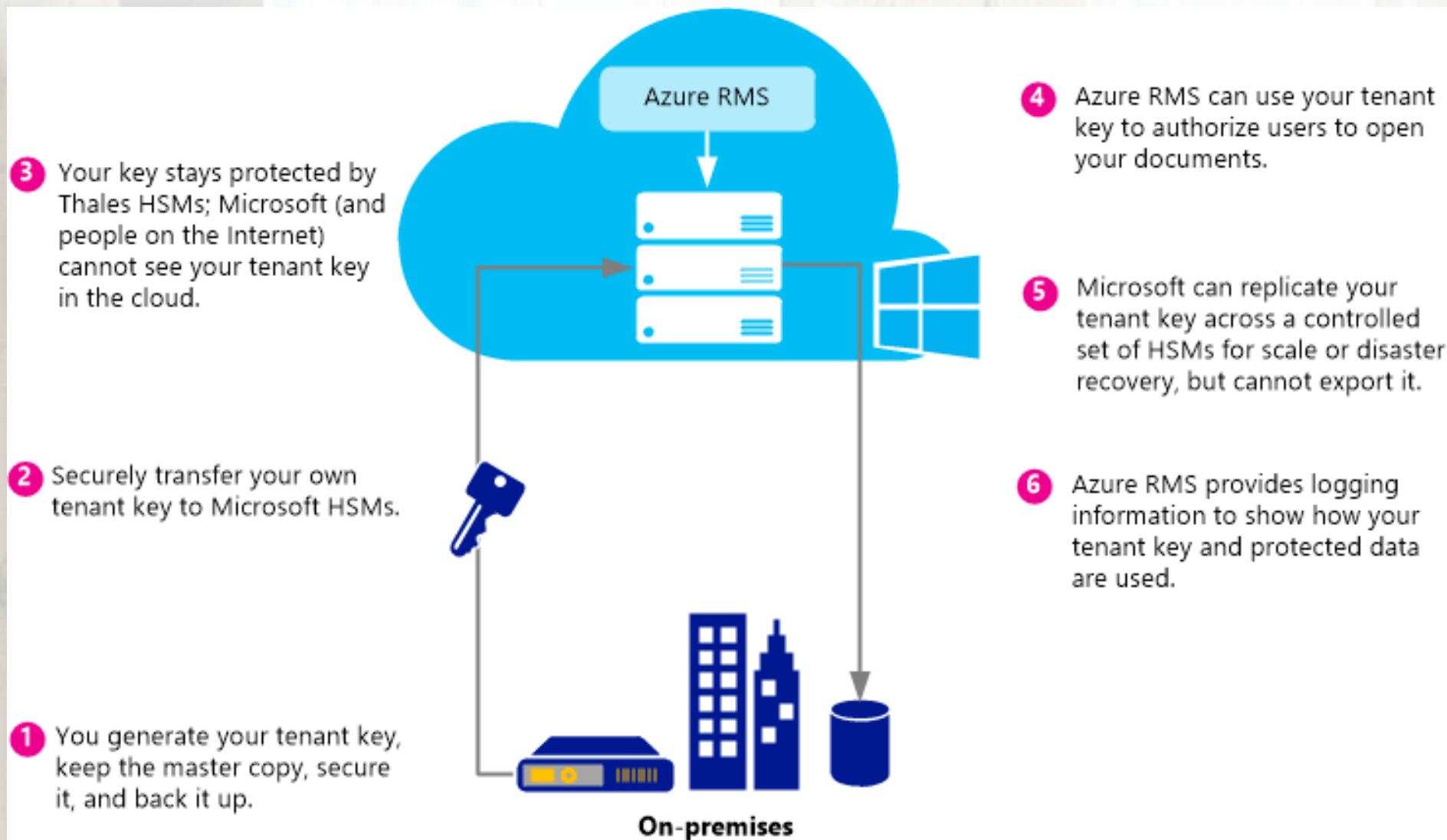
A partir de 2016

Cifrado de contenido (Rights Management)

Información
puede enviarse
protegida o
hacerlo en
tránsito usando
reglas



Cifrado de contenido (BYOK)



Customer Lockbox

OPERANDO A GRAN ESCALA

Millones de usuarios

Datacenters en distintas regiones

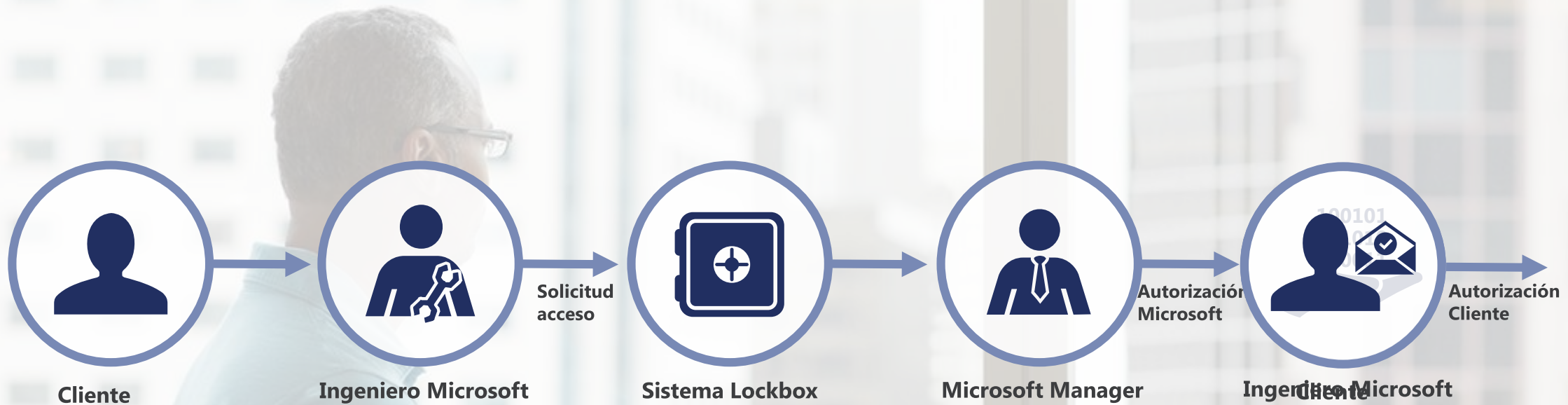
100s de miles de servidores

Siempre actualizado

Alta fiabilidad (99.99% en Q1 2015)



Customer Lockbox



El cliente controla el acceso a su información

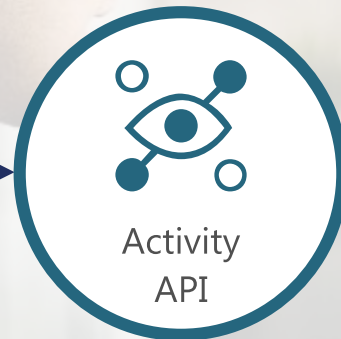
Trazabilidad



Outlook			Calendar	People	Newsfeed	SkyDrive	Sites	...	Admin	Administración
correo										
Buzones activos e inactivos			Buzones nuevos y eliminados			Grupos nuevos y eliminados				
Uso del buzón			Tipos de conexiones de buzón							
USO										
Explorador utilizado			Sistema operativo utilizado			Licencias frente Uso activo				
Lync										
Usuarios activos			Sesiones de punto a punto			Conferencias				
Minutos de audio y minutos de vídeo			Dispositivos cliente							
SharePoint										
Métricas de almacenamiento de los inquilinos			Sitios de grupo implementados			Almacenamiento de sitio de grupo				
OneDrive para la Empresa										
Sitios de OneDrive para la Empresa implementados			Almacenamiento de OneDrive para la Empresa							
auditoría										
acceso al buzón de correo por parte de usuarios no propietarios			cambios de grupo de funciones			búsqueda y retención de contenido del buzón de correo				
retenciones de buzones de correo por juicio			Informes de Azure AD							
protección										
principales remitentes y destinatarios			malware más frecuente para el correo			detecciones de malware				
detecciones de spam			correo enviado y recibido							
reglas										
principales coincidencias con la regla para el correo			coincidencias con la regla para el correo							
DLP										
principales coincidencias con la directiva DLP para el correo			principales coincidencias con la regla DLP para el correo			coincidencias con la directiva DLP por severidad para el correo				
coincidencias con la directiva DLP, coincidencias con la directiva DLP, coincidencias con la directiva DLP										

Informes, logs, auditoría

API de actividad



ISVs

RAPID7

palerra

sumologic

ALERTLOGIC
Security. Compliance. Cloud.

CloudLock

BetterCloud
Powering CloudIT

logentries™

AvePoint®

cogmotive
Office 365 Reports

VARONIS

netskope

skyhigh

druva

LogRhythm

Seguridad con Windows 10

Credential
Guard



Microsoft
Passport



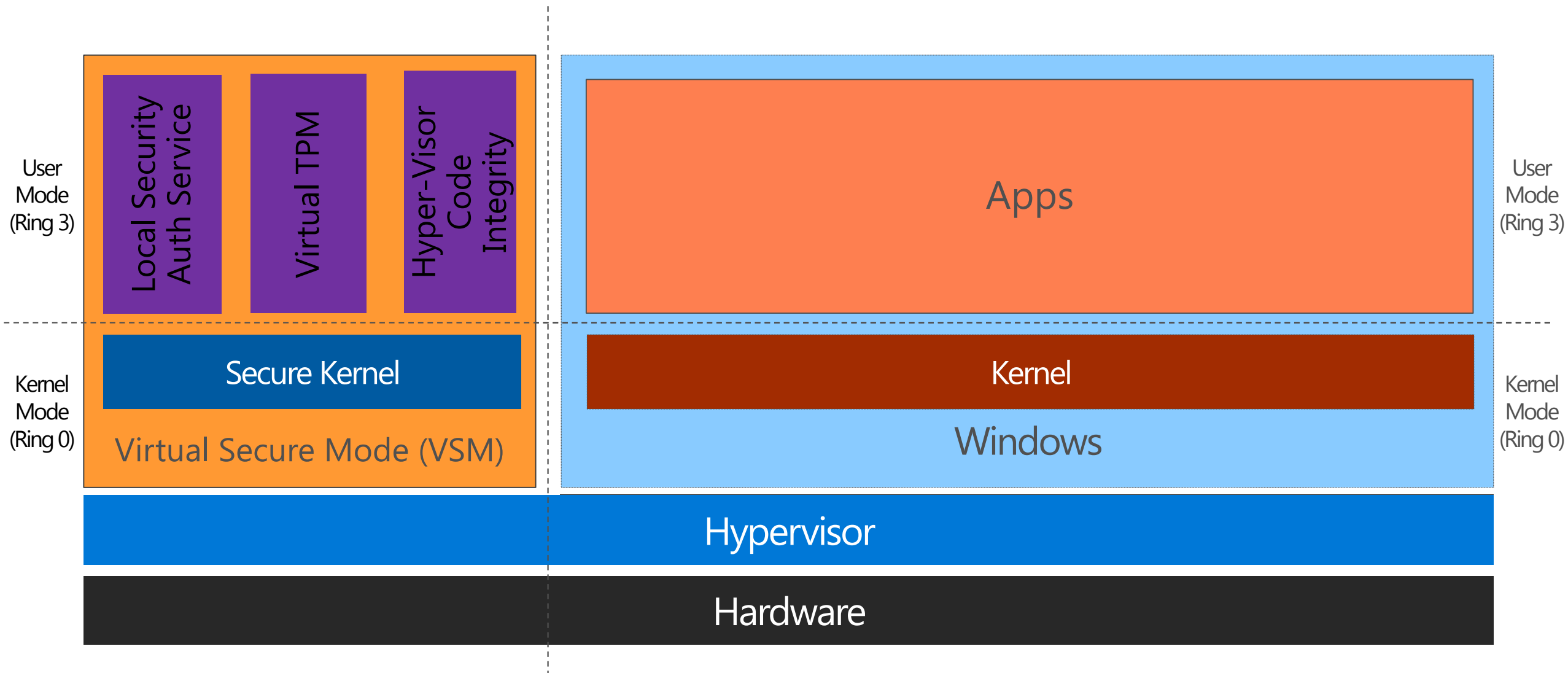
Device
Guard



Credential Guard

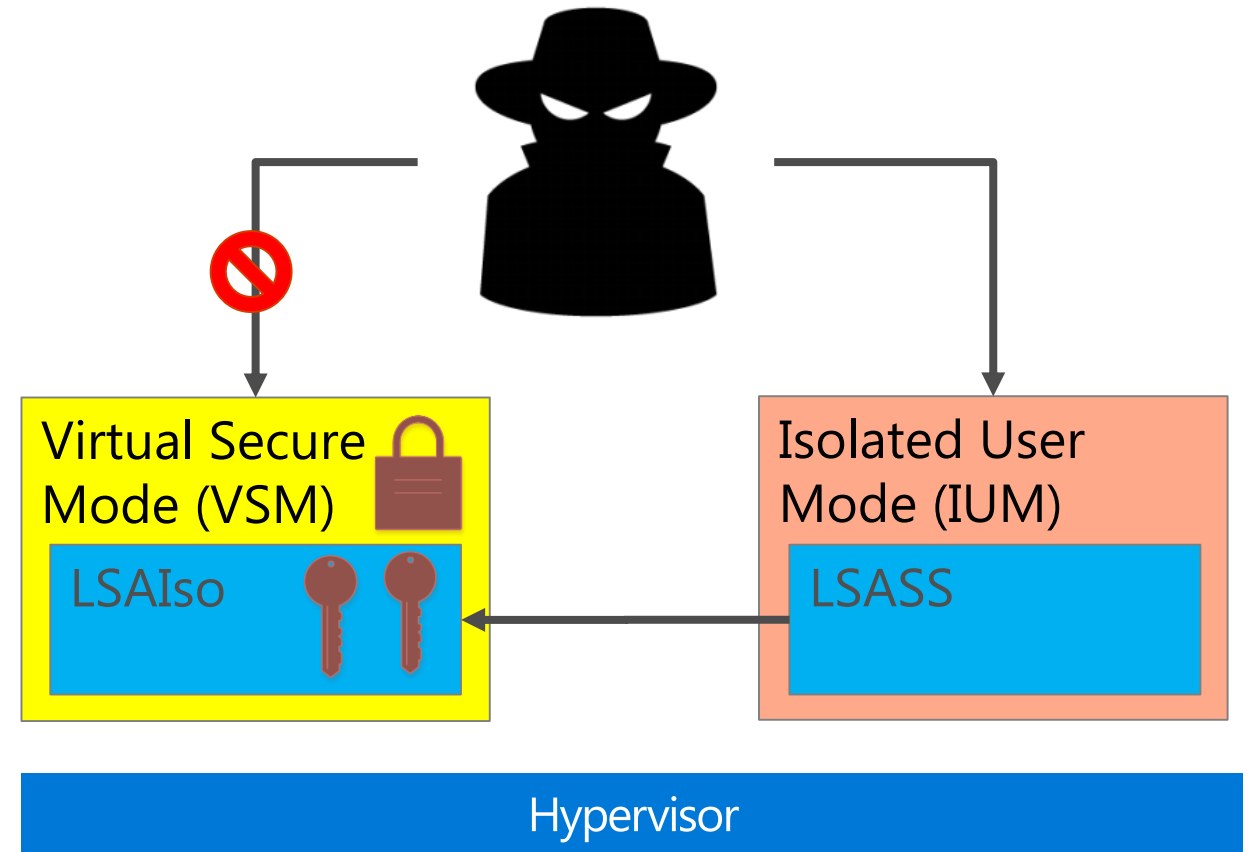


Arquitectura Virtual Secure Mode (VSM)



Las credenciales estarán "aisladas"

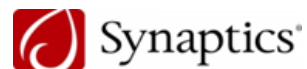
Protegerse de ataques tipo
Pass-the-Hash o Pass-the-
Ticket



Microsoft Passport



FIDO Alliance



REGISTRATION BEGINS

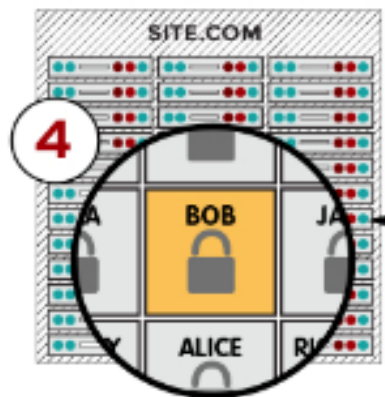


USER APPROVAL



USER APPROVAL

REGISTRATION COMPLETE



Using
PUBLIC KEY
CRYPTOGRAPHY

NEW KEY CREATED



KEY REGISTERED

LOGIN

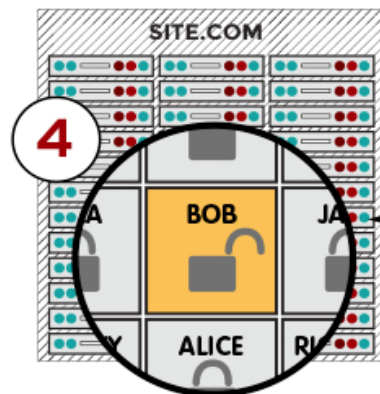


USER APPROVAL



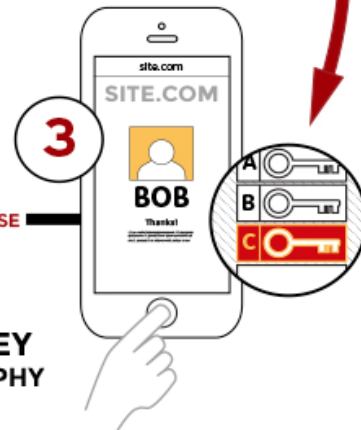
LOGIN CHALLENGE

LOGIN COMPLETE



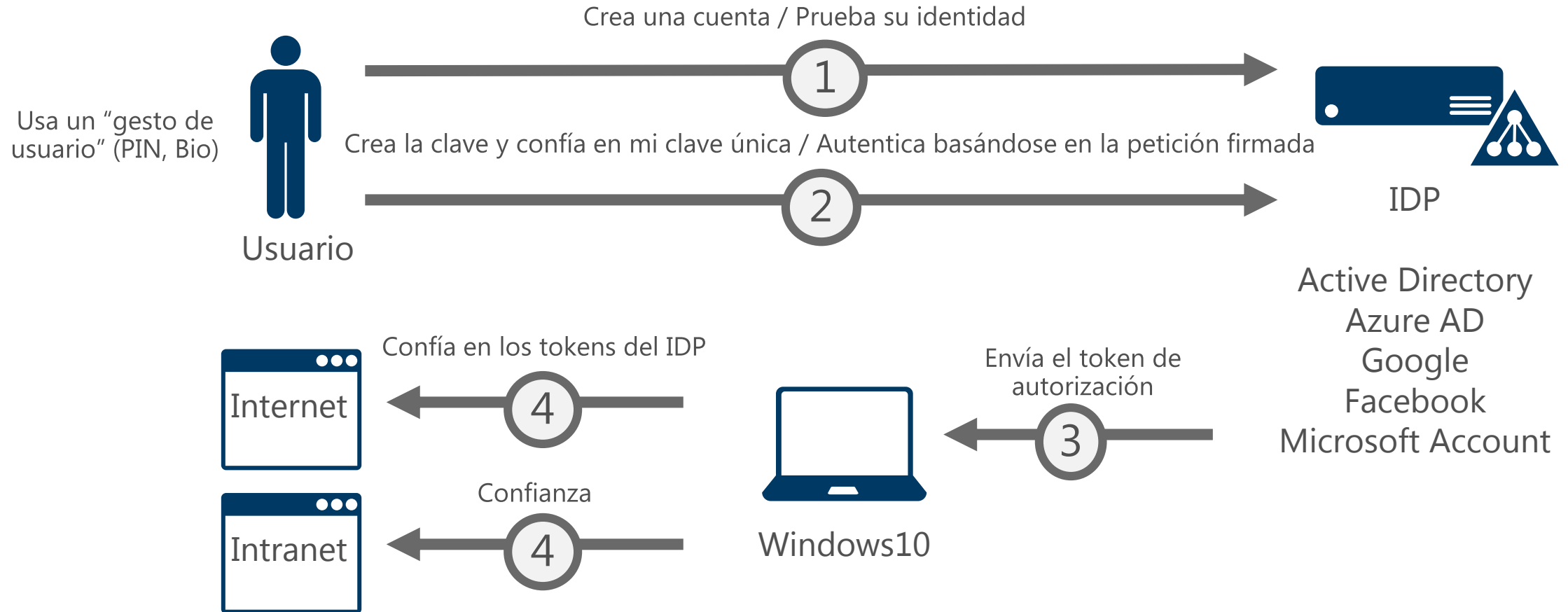
Using
PUBLIC KEY
CRYPTOGRAPHY

KEY SELECTED



LOGIN RESPONSE

Microsoft Passport

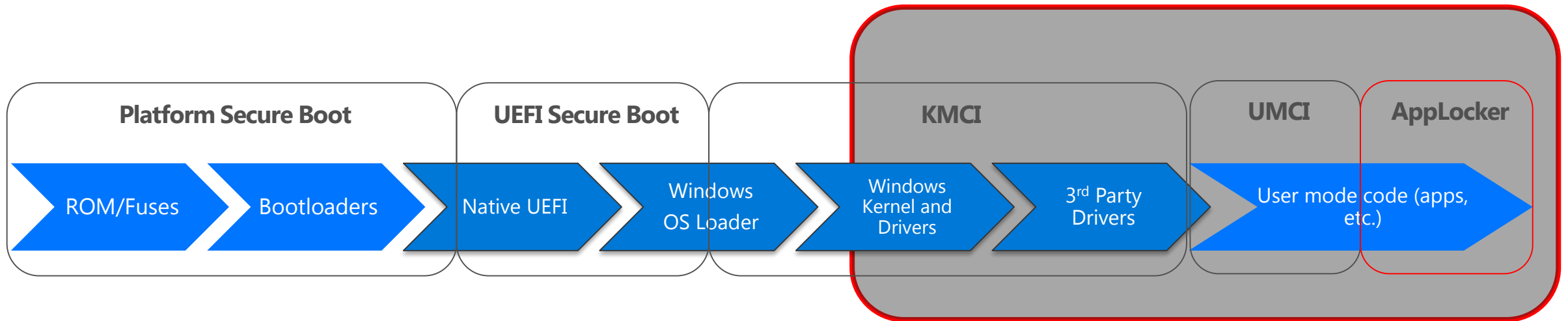


Device Guard

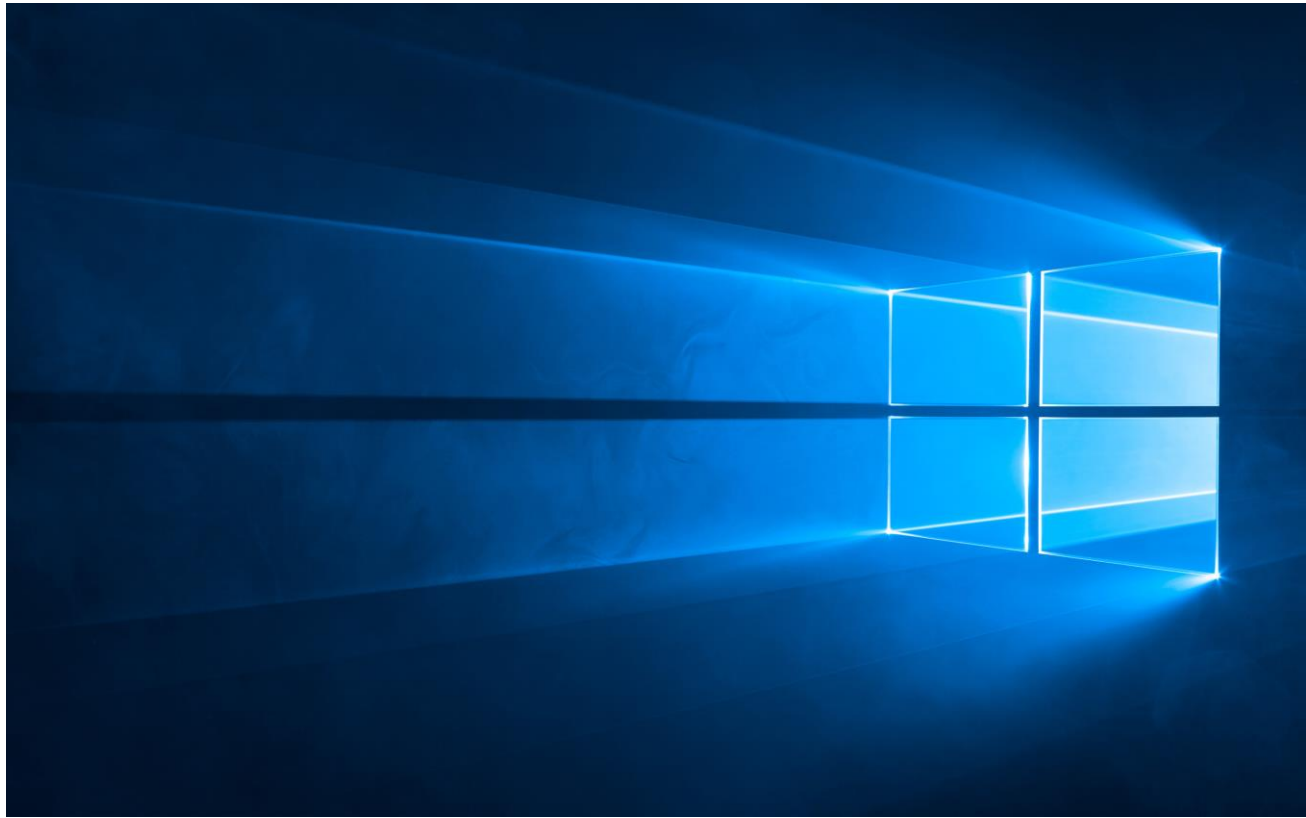


Control de Integridad desde el arranque

Si la aplicación no es confiable, no se ejecutará.



Y mucho más ...



Windows Hello

AppLocker

BitLocker

Enterprise Data Protection

Device Management

Lockdown

Security Auditing

