Adaptive Defense

INFORMACIÓN ENVIADA Y CERTIFICACIONES DE AZURE

panda

pandasecurity.com

01 ¿Qué información es enviada/guardada en la nube?

02 ¿Se comparte algún tipo de información con terceros?

03 ¿La información se envía encriptada?

04 ¿Qué seguridad tiene la plataforma donde se alojan los datos?

05 ¿Qué certificaciones de seguridad tiene la plataforma donde se alojan los datos?

06 ¿Dónde está ubicada la plataforma de Windows Azure?

01

¿Qué información es enviada/ guardada en la nube?

En este apartado se muestra la información que es enviada a la nube por los agentes de Adaptive Defense que se instalan en cada Endpoint para ofrecer una garantía de protección completa en portátiles, estaciones y servidores Windows.

El nuevo modelo de protección de Adaptive Defense requiere recoger información de lo que hacen las aplicaciones. La continuación monitorización de las acciones realizadas por las aplicaciones y el posterior análisis de estos datos con técnicas de machine learning en nuestros entornos Big data es lo que nos permite ofrecer una protección de garantías a nuestros clientes.

Los datos recogidos por el servicio Adaptive Defense siguen las siguientes directrices:

- Se recoge únicamente información relativa a ficheros ejecutables de Windows, (fichero .exe, .dll, ...) que se ejecutan / cargan en la máquina.
- Los atributos de dichos ficheros se envían normalizados intentando evitar en lo posible que contengan información referente al usuario logueado. Así por ejemplo las rutas de ficheros se normaliza como LOCALAPPDATA\nombre. exe en lugar de c:\Users\NOMBRE_ DE_USUARIO \AppData \Local\ nombre.exe.
- Las URLS recogidas son únicamente las de descargas de ficheros ejecutables. No se recogen URLs de navegación de usuarios.
- No existe nunca la relación dato-usuario dentro de los datos recogidos.
- En ningún caso Adaptive Defense envía información personal a la nube.

La **información de la regocida de las máquinas** es la siguiente:

- Nombre del equipo.
- Sistema operativo.
- Service Pack. Grupo en el que el PC protegido es incluido.
- IP por defecto de la máquina.
- MAC.
- Direcciones IP asignadas al PC en los diferentes adaptadores de red.
- MAC para los diferentes adaptadores de red.
- Memoria Ram en MB.

Sobre las acciones que realizan las aplicaciones en el sistema

Como información imprescindible para soportar el nuevo modelo de protección de Adaptive Defense se envía **información sobre las acciones que realizan las aplicaciones** en el sistema protegido por Panda Adaptive Defense.

Atributo	Dato	Descripción	Ejemplo
Fichero	Hash	Hash del fichero al que hace referencia el evento	N/A
URL	Url	Dirección desde donde se ha descargado un PE	http://www.malware.com/ejecutable.exe
Path	Path	Ruta normalizada en la que se encuentra el fichero al que hace referencia el evento	APPDATA\
Registro	Clave / Valor	Clave del registro de Windows y su contenido relacionado	HKEY_LOCAL_MACHINE\SOFTWARE\Panda Security\Panda Research\Minerva\Version = 3.2.21
Operación	Id Operación	Identificador de operación realizada en el evento (creación/modificación/carga/.. de ejecutable, descarga de ejecutable, comunicación,...)	El evento de tipo 0 indica la ejecución de un PE
Comunicación	Protocolo /Puerto/ Dirección	Recoge el evento de comunicación de un proceso (no su contenido) junto con su protocolo y dirección	Malware.exe envía datos por UDP en el puerto 4865
Software	Software Instalado	Recoge la lista de software instalado en el endpoint según el API de Windows	Office 2007, Firefox 25, IBM Client Access 1.0

Adicionalmente puede ser necesario enviar ficheros ejecutables a nuestra **plataforma de Inteligencia Colectiva**. Para reducir el consumo de ancho de banda sólo se envían ficheros ejecutables a la plataforma de Inteligencia Colectiva en caso de no estar aún presentes. Al enviarse únicamente ficheros ejecutables nos aseguramos que en ningún caso contendrán información confidencial del usuario / cliente.

02

¿Se comparte algún tipo de información con terceros?

Toda la información con la que se trabaja, se almacena únicamente en nuestra plataforma cloud de Windows Azure.

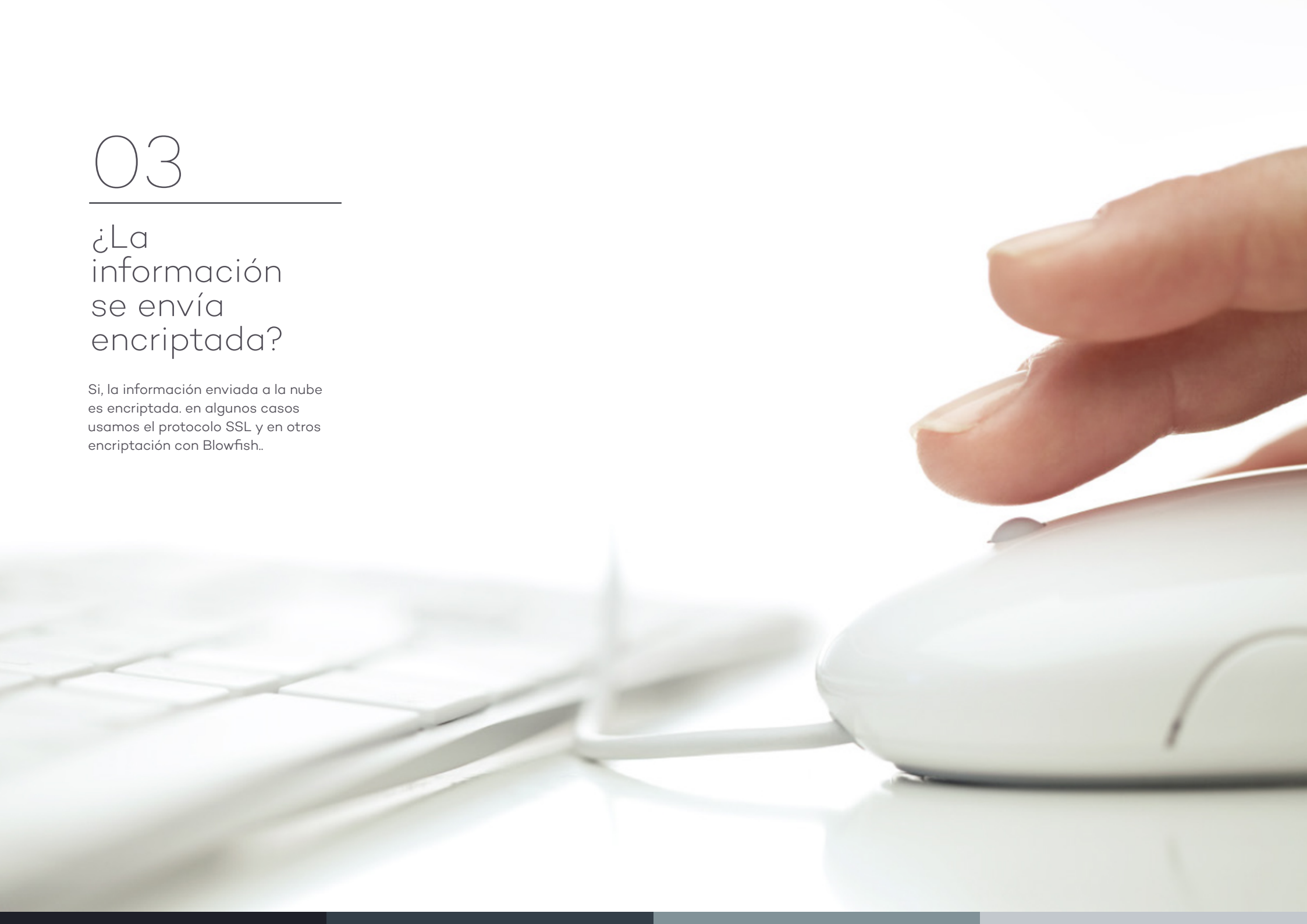
La información no es compartida con terceros salvo en el caso de que los clientes:

- Quieran recibir en su sistema **SIEM** información sobre las alertas y datos de seguridad que son recogidos por Adaptive Defense. La información de seguridad recogida por Adaptive Defense se enviará a los SIEM de los clientes por un protocolo seguro en acuerdo con el cliente.
- Usen la plataforma **LOGTRUST**, el SIEM con el que Adaptive Defense se integra por defecto. Logtrust es una plataforma Big Data en la nube que almacena en tiempo real la información sobre las evidencias recogidas en todos los puestos protegidos por Adaptive Defense. La información es enviada a Logtrust por HTTPS y se almacena en los CPDs de Logtrust.

03

¿La información se envía encriptada?

Si, la información enviada a la nube es encriptada. en algunos casos usamos el protocolo SSL y en otros encriptación con Blowfish..



04

¿Qué seguridad tiene la plataforma donde se alojan los datos?

Windows Azure, la plataforma donde está alojado Panda Advanced Protection Service, provee la máxima confidencialidad y seguridad de los datos almacenados. Las políticas de seguridad y control establecidas en Azure están descritas en el Whitepaper de “Windows Azure Security Overview”

Windows Azure Security Overview

¿QUÉ SEGURIDAD TIENE LA PLATAFORMA DONDE SE ALOJA LOGTRUST?

Cuenta con las medidas de seguridad física del CPD de Amazon. Podemos ver el detalle en el siguiente link:

AWS Compliance

El acceso a los sistemas de Logtrust siempre está filtrado por Firewall y autenticado con certificados.

Además, todos los sistemas, servicios y aplicaciones que componen la infraestructura cloud reportan sus logs con diversos fines entre ellos los de auditoría y seguridad.

05

¿Qué certificaciones de seguridad tiene la plataforma donde se alojan los datos?

Tal y como se indica en el .pdf del apartado anterior Windows Azure corre sobre Microsoft Global Foundation Services (GFS): "Windows Azure operates in the Microsoft Global Foundation Services (GFS) infrastructure".

El siguiente documento muestra información sobre la gestión de la seguridad que se hace en Global Foundation Services (GFS), la infraestructura Cloud de Microsoft en la cual corre Windows Azure:

Microsoft's cloud services

En el .pdf se indican las certificaciones de Windows Azure:

- **ISO/IEC 27001:2005**
- Statement on Auditing Standards No. 70 **(SAS 70)** Type I and II
- Sarbanes-Oxley **(SOX)**
- Payment Card Industry Data Security Standard **(PCI DSS)**
- Federal Information Security Management Act **(FISMA)**

Adicionalmente tenemos información más detallada sobre la certificación 27001 en:

Windows Azure Achieves ISO 27001

Por último, indicar que en:

Detalles

hay un White Paper que describe como Windows Azure cumple con los requisitos de seguridad definidos por Cloud Security Alliance, Cloud Control Matrix.

Se adjunta párrafo del Whitepaper:

"Our security framework based on ISO 27001 enables customers to evaluate how Microsoft meets or exceeds the security standards and implementation guidelines. ISO 27001 defines how to implement, monitor, maintain, and continually improve the Information Security Management System (ISMS). In addition, the GFS infrastructure undergoes an annual American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) No. 70 audits, which will be replaced with an AICPA Statement on Standards for Attestation Engagements (SSAE) No. 16 audit and an International Standards for Assurance Engagements (ISAE) No. 3402 audit. Planning for an SSAE 16 audit of Windows Azure is underway."

CERTIFICACIONES DE SEGURIDAD DE LA PLATAFORMA DONDE SE ALOJA LOS DATOS DE LOGTRUS

Para aquellos clientes que vayan a hacer uso del servicio Logtrust, deben saber que cuentan con las medidas de seguridad física del CPD de Amazon.

Windows Azure Security Overview

Como se puede ver en detalle accediendo al link anterior, Amazon cuenta con todas las principales certificaciones del mercado destacando:

- **ISO/IEC 27001**
- SOC 1/SSAE 16/ISAE 3402 **(previously, SAS70)**
- Payment Card Industry Data Security Standard **(PCI DSS)**
- Federal Information Security Management Act **(FISMA)**

06

¿Dónde está ubicada la plataforma de Windows Azure?

Windows Azure contiene nodos en diferentes ubicaciones en todo el mundo. Actualmente Panda Security tiene ubicado su datacenter en Irlanda.

Se adjunta foto del datacenter de Irlanda.

¿DÓNDE ESTÁ UBICADA LA PLATAFORMA AMAZON DE LOGTRUST?

Logtrust opera en alta disponibilidad a través de sus plataformas Amazon ubicadas en su datacenter en Irlanda.


panda