**Resumen de las características principales sobre la seguridad del Cloud de Microsoft Azure.**

Evolsystem selecciono la plataforma Cloud de Microsoft Azure como proveedor principal para desplegar nuestras aplicaciones y servicios tecnológicos.  La Plataforma evolPOS se ejecuta completamente en Azure.

La característica de ser una plataforma abierta y flexible que provee todos los servicios para la construcción rápida, despliegue y administración de soluciones basadas en la nube. A la vez que ofrece una amplia gama de servicios basados en uso, a través de aplicaciones, cómputo, almacenamiento y redes. Nos permite construir aplicaciones usando cualquier lenguaje, herramienta o marco en un portal completamente automatizado de auto-servicio que habilita el aprovisionamiento de recursos escalables en minutos.

La seguridad es fundamental en los servicios de aplicaciones y Azure nos ofrece la seguridad multicapa que se proporciona en sus centros de datos con expertos en ciber seguridad que lo supervisan activamente para proteger los recursos y los datos que se utilizan activamente.

Azure es el proveedor de cloud con más certificaciones, hecho que garantiza que la ejecución de los servicios esté construida con la calidad de seguridad y privacidad necesarias.


En el centro de confianza de Microsoft Azure, https://azure.microsoft.com/en-us/support/trust-center/, se puede entrar en más en detalle en estas certificaciones.

## Log de registro de cambios

Además, Azure nos provee de un log de actividades para registrar qué operaciones se realizan sobre los recursos, quién realiza las operaciones, cuando se realizan, el estado de las mismas y las propiedades y valores de los cambios realizados, de los últimos 90 días.

Este log nos provee de una vista de las operaciones que se realizan en los servicios de los grupos de recursos. Por una parte, asegura que no se producen cambios no esperados, y por otra, permite realizar un diagnóstico detallado de los errores de despliegue como herramienta de resolución de problemas.

## Control de acceso a los recursos basada en roles

Azure nos permite establecer control de acceso granular a los recursos de la suscripción utilizando el Role-Based Access Control (RBAC).

Con RBAC asignamos sólo los permisos necesarios para que los usuarios puedan realizar su trabajo. Por ejemplo, podemos dar permisos a un usuario para visualizar los informes web pero que no tenga permisos para modificar la configuración de este servicio.

Cada suscripción está asociada a un Azure Active Directory que RBAC usa para gestionar los usuarios, grupos y aplicaciones. Por defecto, RBAC usa los roles de Owner, Contributor y Reader, pero si fuera necesario, se pueden crear roles personalizados con los permisos necesarios.

El control de acceso se puede aplicar a nivel de Suscripción, grupo de recursos o recurso, con lo que garantizamos la simplicidad de la administración y la granularidad necesaria para dar los permisos adecuados a cada usuario.

## Encriptado de la información sensible

Azure nos ofrece diversos mecanismos para mantener información sensible, por ejemplo, datos personales, encriptada en transporte y en almacenamiento.

- Transport Layer Security / Secure Sockets Layer, que nos permite cifrar simétricamente las comunicaciones, por ejemplo, de los sitios web.
- Microsoft Azure Storage Service Encryption para cifrar la información almacenada en Blob Storage.
- Transparent Data Encryption, tecnología que permite encriptar la información de las bases de datos de Azure SQL de forma transparente a las aplicaciones que tienen que hacer uso de estos.
- Azure Key Vault, servicio que ofrece la capacidad de administrar las claves de encriptación y/o de almacenar de forma segura y encriptar los valores de configuración de las aplicaciones web, usando una versión cloud de HSM (Hardware Security Module).

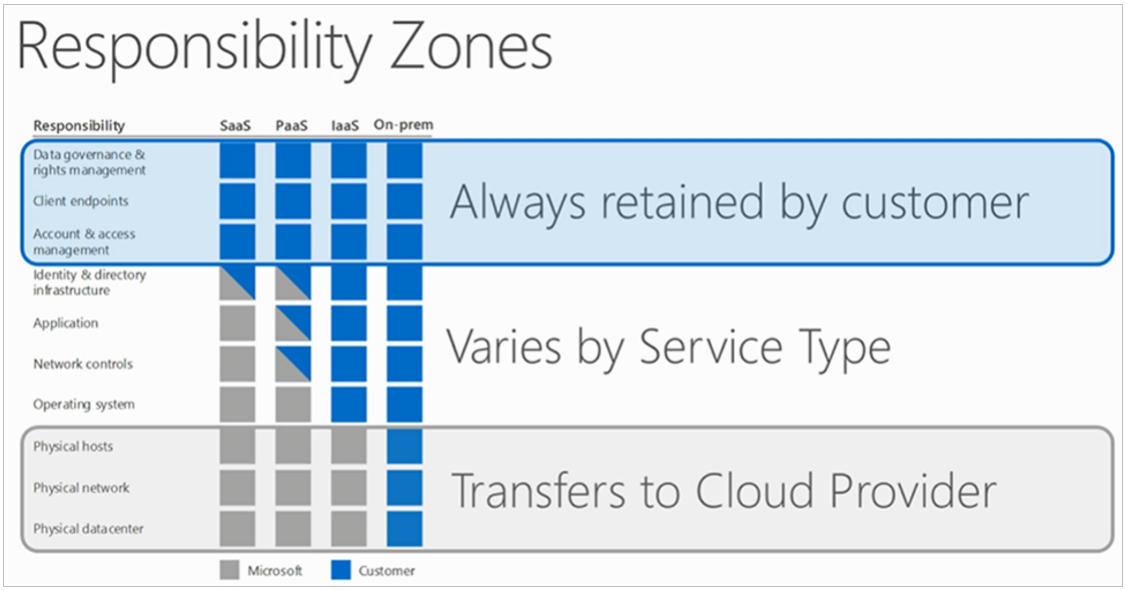
### Seguridad en las comunicaciones

Azure App Service, el servicio PaaS de aplicaciones de Azure, administra la seguridad a nivel de infraestructura y plataforma, en los siguientes puntos básicos:

- Las aplicaciones se ejecutan en un entorno aislado seguro
- Las comunicaciones entre recursos de Azure se ejecutan en la red segura de Azure y no cruzan redes públicas, además de ser comunicaciones encriptadas.
- La protección de recursos ante amenazas del tipo malware, DDoS, Man-in-the-middle y otras amenazas está activa las 24 horas del día.
- Las actualizaciones del sistema operativo son gestionados por el equipo de operaciones de Azure.

Si fuera necesario, podemos aumentar el nivel de seguridad que nos ofrece por defecto Azure, utilizando Azure Application Gateway configurado como Web Application Firewall (WAF) que nos ofrece una protección centralizada contra las vulnerabilidades de seguridad más comunes:

- SQL injection
- Cross site scripting
- Ataques web comunes (Command injection, HTTP request smuggling, HTTP response splitting, remote file inclusion)
- HTTP protocol violations
- HTTP protocol anomalies (missing host user-agent, …)
- Bot, crawlers and scanners




Todas estas reglas, configurables, están basadas en el conjunto de reglas OWASP (Open Web Application Security Project).

Esperamos que este breve resumen sobre la seguridad entregada por el Cloud de Microsoft Azure, ayude a un mejor entendimiento entre cliente y proveedor.

Para más información sobre la seguridad del Cloud de Microsoft Azure visite:
https://azure.microsoft.com/es-es/overview/trusted-cloud/

Gracias

**Ivan C. Muñoz H.**
Director de Proyectos de Evolsystem
Julio 2019