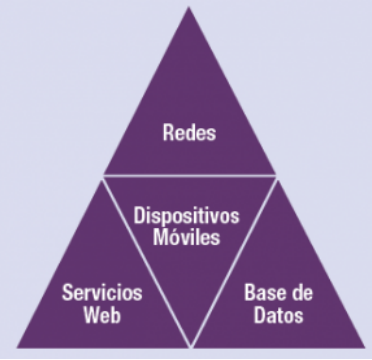
Los distintos controles de auditoría para los pagos móviles

Una vez vistos los múltiples riesgos existentes en los pagos móviles, debemos concienciar a todos sus usuarios a prevenirlos de manera que no se lleven las manos a la cabeza, por lo tanto, en la presente entrada describiremos los diferentes controles de auditoría que se deberán realizar para hacer un correcto uso de esta tecnología y correr los menores riesgos posibles.

La primera tarea que debe realizarse es definir los principales segmentos de riesgo de las aplicaciones de pagos móviles, de esta manera, será más fácil establecer un control más ordenado y en buenas condiciones. Tal y como aporta ISACA y se muestra en la imagen adjuntada en la parte inferior del presente párrafo, los 4 segmentos de riesgos básicos son las redes móviles, dispositivos móviles, servicios web y bases de datos, por lo que, a continuación, se incluirá una tabla en la que se detallan los controles clave para garantizar y fortalecer la seguridad en las apps móviles.



Área	Tema que controlar	Controles	Riesgo mitigado

Dispositivos móviles	Almacenamiento de datos	Cifrado de dicha información mediante estándares como 128, 192 o 256.	Pérdida de datos
Dispositivos móviles	Transmisión de datos	Aplicar la encriptación de datos, así como diferentes protocolos de seguridad como HTTPS, TLS, FTPS.	Pérdida de datos
Dispositivos móviles	Ingeniería inversa del código de la aplicación	Uso de protecciones binarias.	Pérdida de datos, acceso no autorizado
Dispositivos móviles	Acceso a la aplicación y seguridad	Uso de gestor de aplicaciones MAM que gestione el acceso y despliegue de la app. Algunos ejemplos son MobileIron o Airwatch	Acceso no autorizado y fraude
Redes móviles	Conectividad inalámbrica	Transmisión de datos mediante protocolos criptográficos seguros como SSL o TLS.	Pérdida y revelación de datos

Redes móviles	Secuestro de sesión	Las conexiones de las a través de TLS son a través de HTTPS en lugar de HTTP, de esta manera, nos aseguramos de conectarnos a una URL.	Acceso no autorizado, pérdida de datos y revelación de estos
Redes móviles	Suplantación de identidad	Uso de protocolos de comunicación segura TLS, Secure Shell (SSH) y HTTPS.	Acceso no autorizado y pérdida de datos
Servicios Web	Parche de operaciones para la administración	Uso de procesos para el despliegue e identificación de parches del sistema.	Pérdida de datos y acceso no autorizado
Servicios Web	Gestión de acceso	Roles correspondientemente definidos y cada uno con los accesos específicos.	Pérdida de datos y acceso no autorizado
Servicios Web	Ataque de fuerza bruta	Evitar DoS y emplear técnica CAPTCHA de manera que se pueda obtener una clara distinción entre humanos y computadoras.	Fraude y acceso no autorizado

Bases de datos	Acceso privilegiado	Limitar acceso a la base de datos y llevar un exhaustivo control de las contraseñas del sistema.	Fraude y acceso no autorizado
Bases de datos	Inyección SQL	Para cada tipo de sintaxis habrá unas reglas plenamente definidas con su respectiva valoración.	Fraude y acceso no autorizado
Bases de datos	Validación de la entrada de la app	Uso de diferentes controles de lógica para una correcta protección	Fraude y acceso no autorizado
Bases de datos	Servicios de aplicaciones de BBDD	Uso obligatorio de conexiones SSL, uso de HTTPS para el logeo de la app y un servidor de BBDD correctamente probado.	Fraude y acceso no autorizado

Tal y como habéis visto en la figura situada en la parte superior, el auditor debe ser quien establezca las diferentes áreas a controlar en caso de posibles riesgos. Asimismo, para cada una de esas áreas, será importante señalar los riesgos evitados gracias al uso de éstos [1].

Por otro lado, en la entrada anterior prometí completar una de sus figuras relacionadas con otros muchos posibles riesgos referentes a las apps móviles para el pago, por ello, en la parte inferior se describen sus planes de contingencia correspondientes:

Tipo de objetivo perseguido	**Amenazas**	**Riesgos**	**Controles a realizar**
Usuario	Intercepción del tráfico	Robo de identidad	**Uso de TPM y encriptación**
Usuario	Intercepción de datos de autenticación	Robo de parámetros de autenticación, divulgación de información confidencial	**Autenticación de ambos usuarios (PIN) y firma digital verificado por tercera parte**
Usuario	Enmascaramiento del usuario	Transacciones fraudulentas	**Autenticación de dos factores**
Usuario	Configuración y complejidad de configuración	Reducción en la adopción de la tecnología	**Interfaz de usuario simplificada**
Usuario	Infección del dispositivo móvil	Divulgación de datos y violación de la privacidad	**Control de usuario de las características de geolocalización, privacidad criptográficamente apoyada.**
Proveedor de servicio	Ataques enmascarados	Robo de servicios y modificación de mensajes	**Solicitar filtrado en base al lector en dispositivo móvil**

Proveedor de servicio	Distribución ilegal de contenido como videos o juegos.	Robo de contenido, piratería digital.	**Incorporación de DRM en el Smartphone**
Proveedor de servicio	Modificación de mensajes, respuesta de transacciones.	Robo de servicio o contenido, pérdida de ingresos, transferencia ilegal de fondos	**Uso de protocolos criptográficos potentes y autenticación vía SMS**

Como ya se ha dicho en diversas ocasiones, estamos tratando con una de las tecnologías que más riesgos corren del mercado actual, por ello, la tabla 2 muestra algunos otros riesgos que también podemos correr al hacer uso de todo ello. Igualmente, el impacto que estos pueden causar es también objeto de investigación, luego, el auditor deberá priorizar cada uno de ellos en función de estos valores [2], tarea que ya se realizó en la entrada previa.

Con toda la información ya adjuntada podemos afirmar que los auditores de las tecnologías de la información son una pieza clave ya que deben de encargarse de realizar un proceso de vigilancia de manera que exista un control en situaciones de riesgo como las enumeradas en las ilustraciones anteriores. Además, deben de encargarse de las llamadas pruebas de penetración (práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar) cada vez que las aplicaciones sean actualizadas [3].

A modo de recapitulación, hasta el momento hemos descrito el

marco general de las aplicaciones móviles para el pago, su impacto en la industria, los riesgos que conlleva su uso y, gracias a este último, ya sabemos la manera en la que poder solventarlos. Aun así, creo que es relevante exponer el futuro de éstas apps que todo utilizamos, de manera que conozcamos todo lo que se nos viene por delante y afrontarlo de la mejor manera posible.

Bibliografía

[1] Journal volume 4 2016 spanish Issues. Acceso el 08/10/18. https://www.isaca.org/Journal/archives/2016/volume-4/Documents/Journal-volume-4-2016-Spanish.pdf

[2] Mobile Payments: Risk, Security and Assurance Issues. Acceso el 09/10/18. https://www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/MobilePaymentsWP.pdf

[3] Prueba de penetración. Acceso el 12/10/2018. https://searchdatacenter.techtarget.com/es/definicion/Prueba-de-penetracion-pen-test