Drones: controles y auditoría

En el post anterior realicé un análisis de los riesgos que implica el uso de drones, evaluando si son altos, medios o bajos teniendo en cuenta la probabilidad de ocurrencia y la gravedad de las consecuencias en caso de que el riesgo se materialice.

Con el objetivo de completar dicho análisis, en este post voy a definir los controles que deberían llevarse a cabo para mitigar los riesgos identificados, tanto los no intencionados como los intencionados. Asimismo, hablaré sobre el rol del auditor en relación con los drones.

Controles

Riesgos no intencionados

Los controles para los riesgos no intencionados se basan en verificar que se cumple con el Real Decreto 1036/2017 que regula el uso de drones en España [1], el cual ya traté en un post anterior.

Teniendo en cuenta que la normativa no se aplica de igual manera cuando el dron se usa de forma recreativa o profesional, también he realizado esta separación en la descripción de los controles.

Riesgos	Controles para uso recreativo	Controles para uso profesional
Daños a edificios	• Verificar que no se vuela sobre aglomeraciones de edificios. • Verificar que no se vuela de noche si el dron pesa más de 2 kg. • Verificar que se encuentra al alcance de la vista y que no se vuela a más de 120 m del suelo.	• Verificar el seguro de responsabilidad civil, la habilitación en AESA[1], si es piloto de RPAS[2] y si tiene el certificado médico en vigor. • Verificar la autorización para volar sobre aglomeraciones de edificios. • Verificar la autorización para volar en BVLOS[3] con un dron de más de 2 kg. • Verificar la autorización para volar de noche.
Daños a aeronaves	• Verificar que no se vuela de noche si el dron pesa más de 2 kg. • Verificar que no se vuela a un mínimo de 8 km de aeropuertos y similares. • Verificar que no se vuela en Espacio Aéreo Controlado ni donde se realicen otros vuelos a baja altura. • Verificar que se encuentra al alcance de la vista y que no se vuela a más de 120 m del suelo.	• Verificar el seguro de responsabilidad civil, la habilitación en AESA[1], si es piloto de RPAS[2] y si tiene el certificado médico en vigor. • Verificar la autorización para volar a menos distancia de la que marca la Ley en las proximidades de aeropuertos y similares. • Verificar la autorización para volar en Espacio Aéreo Controlado y Zonas de Información de Vuelo. • Verificar la autorización para volar en BVLOS[3] con un dron de más de 2 kg. • Verificar la autorización para volar de noche.

Riesgos	Controles para uso recreativo	Controles para uso profesional
Daños a personas	• Verificar que no se vuela sobre personas. • Verificar que no se vuela de noche si el dron pesa más de 2 kg. • Verificar que se encuentra al alcance de la vista y que no se vuela a más de 120 m del suelo.	• Verificar el seguro de responsabilidad civil, la habilitación en AESA[1], si es piloto de RPAS[2] y si tiene el certificado médico en vigor. • Verificar la autorización para volar sobre grupos de personas. • Verificar la autorización para volar en BVLOS[3] con un dron de más de 2 kg. • Verificar la autorización para volar de noche.
Interferencias	• Verificar que no se vuela a un mínimo de 8 km de aeropuertos y similares. • Verificar que para la comunicación, se utilizan bandas libres.	• Verificar el seguro de responsabilidad civil, la habilitación en AESA[1], si es piloto de RPAS[2] y si tiene el certificado médico en vigor. • Verificar la autorización para volar a menos distancia de la que marca la Ley en las proximidades de aeropuertos y similares. • Verificar la autorización para volar en Espacio Aéreo Controlado y Zonas de Información de Vuelo. • Verificar que para la comunicación, se utilizan bandas libres.

[1] AESA (Agencia Estatal de Seguridad Aérea)

[2] RPAS (Remotely Piloted Aircraft System)

[3] BVLOS (Beyond Visual Line of Sight)

Riesgos intencionados

Los riesgos intencionados, a diferencia de los no intencionados, no se centran en verificar el cumplimiento de la normativa sino en intentar que ese riesgo no se lleve a cabo. Estos riesgos, debido al objetivo de causar daño que tienen, son más difíciles de controlar. Asimismo, los controles para intentar mitigarlos varían mucho dependiendo del riesgo.

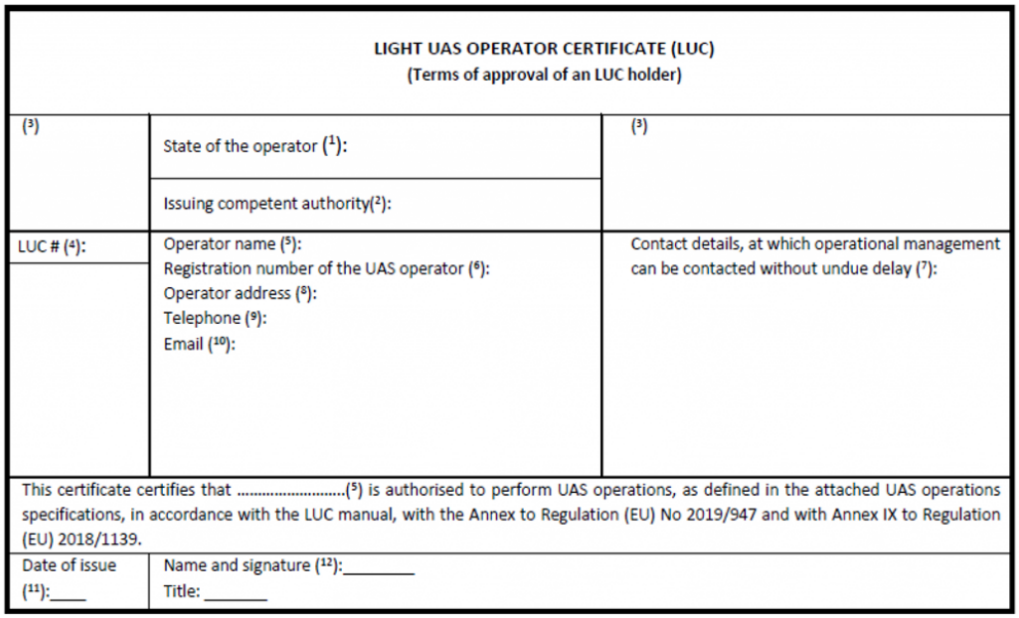
Riesgo	Controles
Ataque terrorista	• Vigilar visualmente el espacio aéreo cercano a zonas susceptibles de ser atacadas. • Rastrear la compra de drones por parte de posibles grupos terroristas.
Ataque de ciberseguridad	• Verificar la dificultad de robar físicamente los datos almacenados en el dron. • Verificar que los datos almacenados en el dron están cifrados. • Verificar que la clave secreta es compleja y larga. • Verificar que las conexiones de la comunicación están cifradas.
Dispersión químico-biológica	• Verificar el contenido de los pulverizadores agrícolas para comprobar que no ha sido modificado. • Vigilar visualmente el espacio aéreo cercano a grupos grandes de personas susceptibles de ser atacadas.

Riesgo	Controles
Contrabando	• Vigilar visualmente el espacio aéreo cercano a las cárceles y fronteras. • Vigilar las inmediaciones de las cárceles y fronteras para comprobar que no hay pilotos de drones.
Violación de privacidad	• Vigilar visualmente el espacio aéreo cercano a la propiedad privada que se quiere proteger. • Ocultar información sensible que puede ser captada por un dron. • Controlar los obstáculos físicos (vallas, barreras, …) que evitan el acceso a la propiedad privada que se quiere proteger.

Rol del auditor

Los drones son una tecnología relativamente nueva y su mercado es cada vez más popular, lo que requiere una supervisión para controlar que se cumple con la normativa vigente y que no suponen un peligro para la sociedad.

Por lo tanto, es imprescindible el rol del auditor para llevar a cabo controles como los descritos en este post. De hecho, las operadoras de drones que quieran obtener un certificado LUC (Certificado de operador de drones ligeros) deben tener un gerente responsable, además de un responsable de monitoreo que lleve a cabo un proceso continuo de auditorías. Este monitoreo puede ser realizado por personal interno o externo. [2]



LIGHT UAS OPERATOR CERTIFICATE (LUC)
(Terms of approval of an LUC holder)

(3)	State of the operator (1): Issuing competent authority(2):	(3)
LUC # (4):	Operator name (5): Registration number of the UAS operator (6): Operator address (8): Telephone (9): Email (10):	Contact details, at which operational management can be contacted without undue delay (7):
This certificate certifies that .....(5) is authorised to perform UAS operations, as defined in the attached UAS operations specifications, in accordance with the LUC manual, with the Annex to Regulation (EU) No 2019/947 and with Annex IX to Regulation (EU) 2018/1139.		
Date of issue (11):____	Name and signature (12):_____ Title: _____	

En definitiva, como en muchas otras tecnologías emergentes, la presencia del auditor es indispensable. Asimismo, el tener que auditar una tecnología nueva evidencia el hecho de que la auditoría es un trabajo interdisciplinar y que requiere la adquisición de nuevos conocimientos según pasan los años y las tecnologías evolucionan. [3]

Referencias

[1] <<Normativa de Drones en España 2020>>, One Air, acceso el 5 de noviembre de 2020, https://www.oneair.es/normativa-drones-espana-aesa.

[2] <<Auditoría de operadoras de drones y certificado LUC>>, Drone Europa, acceso el 5 de noviembre de 2020, https://www.droneuropa.com/auditoria-drones/.

[3] <<The Practical Aspect: Today's Interdisciplinary Auditors>>, ISACA, acceso el 5 de noviembre de 2020, https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/todays-interdisciplinary-auditors.

Controles sobre los dispositivos móviles en la empresa

En el último artículo contemplábamos los riesgos potenciales que implican las tecnologías móviles aplicadas al mundo laboral. Por lo tanto en este artículo analizaremos medidas que nos pueden ayudar a reducir la probabilidad de sufrir daños por culpa de las posibles vulnerabilidades que tengamos en la empresa, así como el rol que deberá adoptar un auditor de tecnologías móviles.

De cara a recordar algunos de los riesgos de los que hablábamos en el artículo anterior, vamos a hacer un breve repaso de ellos:

- SSOO vulnerables
- Skimming
- Escuchas telefónicas
- Lectura de mensajes
- Localización GPS
- Control remoto
- Redes poco seguras
- Ingenieria social

Puesto que actualmente las empresas trabajan manejando información (ya sea esta interna o externa), cualquier de ellas debería tener mecanismos para realizar una gestión adecuada y segura de la información con la que trabajan. Para ello existe la ISO 27001 [1] que especifica una norma para el trato seguro de la información. De todas formas, no es de obligado cumplimiento por lo que muchas empresas aún no lo aplican a su funcionamiento.

El uso de la tecnología móvil en el trabajo se puede implementar desde dos enfoques diferentes: BYOD (Bring Your Own Device) o COPE (Company-Owned, Personally-Enabled). Como afirma el Director de Ciberseguridad de KPMG, una de las Big Four, “las empresas están alentando ampliamente a BYOD. […] Este mundo móvil en rápida evolución presenta nuevos retos para las empresas que gestionan o proporcionan aplicaciones móviles. La integración y la seguridad de las aplicaciones móviles son dos grandes retos para muchas empresas”. Además, también comenta la necesidad de una mayor especialización en tecnologías móviles [2]. Quizás la velocidad a la que ocurren los cambios o la inmensa cantidad de posibilidades que proporcionan los dispositivos móviles sean la razón por la que tienen tanta necesidad de controles.

El problema de la tecnología móvil es que nunca podremos asegurar un uso 100% correcto por parte de los usuarios. Es por eso por lo que la mayor medida de control sobre esta tecnología sea implantar políticas internas de uso que especifique buenas prácticas que los empleados deberán seguir para evitar, en la medida de lo posible, incidentes y disminuir riesgos. Estas políticas se pueden utilizar tanto para la estrategia BYOD como para COPE pero hay riesgos que son difíciles de evitar, por lo que, además de establecer políticas, es necesario tomar otro tipo de medidas.

Entre las recomendaciones recogidas por ISACA en uno de sus artículos se encuentran los programas de formación y concienciación (junto con la involucración de los empleados en la definición y el control de la seguridad), aseguramiento frente a fallos en la seguridad, monitorización de proveedores, securizar las comunicaciones remotas y securización de los dispositivos y sus contenidos [3]. Puede que estas últimas recomendaciones sean, junto con la reducción de costes, las razones por las que KPMG ha pedido a sus empleados que devuelvan sus teléfonos móviles de trabajo. Añaden que tras las inversiones del último año en tecnologías que permiten a sus empleados trabajar desde casa o desde la oficina con tranquilidad, no será tan necesario disponer de teléfonos móviles [4].

Esta medida aborda dos problemáticas potenciales, los usos indebidos de la tecnología y la falta de configuración. La empresa se asegura de que los usuarios dispongan de menos dispositivos que puedan servir de puerta de entrada para posibles atacantes y al mismo tiempo, invierte en la creación y adecuación de sistemas adaptados a las necesidades de la empresa y de sus empleados con la finalidad de ofrecer un servicio íntegro, seguro y disponible desde cualquier localización. De todas formas, las redes a través de las que se comunican los empleados con la empresa siguen siendo un terreno sin securizar si la comunicación se hace de manera remota. Sin embargo, si la empresa dispone una red privada protegida de la red global estará añadiendo una capa más de seguridad a su sistema basado en dispositivos móviles.

El rol del auditor en el ámbito de los dispositivos móviles está expuesto a una gran cantidad de campos en los que profundizar. Uno de los controles a tener en cuenta a la hora de auditar procesos que involucren a la tecnología móvil es el de control de inventario. Una empresa que pierda un dispositivo móvil desde el que se accede a sus sistemas vería seriamente comprometida su integridad si el dispositivo cayese

en manos equivocadas. Lo que sugiere un modelo de auditoria sobre la seguridad de los dispositivos es generar un inventario con los dispositivos que sean propiedad de la empresa, de propiedad privada y propiedad del contratista autorizados para el trabajo con información de la empresa X [5]. Pero, no sólo es necesario auditar los dispositivos de esta manera, sino que también hace falta analizar los controles que se aplican a su uso, los accesos que les están permitidos en los sistemas empresariales, su configuración de seguridad, … Y para todo esto el auditor de dispositivos móviles deberá ser una persona con conocimientos del mundo de las tecnologías móviles si se pretende realizar un estudio exhaustivo y eficaz. De otra manera, es posible que haya ámbitos que se dejen sin revisar y puedan ser objeto de vulneraciones.

[1] ISOTools: ISO 270001 – Sistemas de Gestión de Riesgos y Seguridad, https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/ (30/11/19)

[2] KPMG: Security challenges of mobile devices and applications, *Matthias Bossardt | Partner, 16 March 2016*, https://home.kpmg/ch/en/blogs/home/posts/2016/03/security-challenges-of-mobile-devices-and-applications.html

[3] ISACA: Mobile Workforce Security Considerations and Privacy, Guy Ngambeket, CISA, CISM, CGEIT, ITIL v3 , PMP, https://www.isaca.org/Journal/archives/2017/Volume-4/Pages/mobile-workforce-security-considerations-and-privacy.aspx (30/11/19)

[4] The Guardian: KPMG UK staff told to hand back work mobiles to cut costs, https://www.theguardian.com/business/2019/sep/30/kpmg-uk-mobiles-cut-staff (01/12/19)

[5] KnowledgeLeader: Portable Computing Device Security

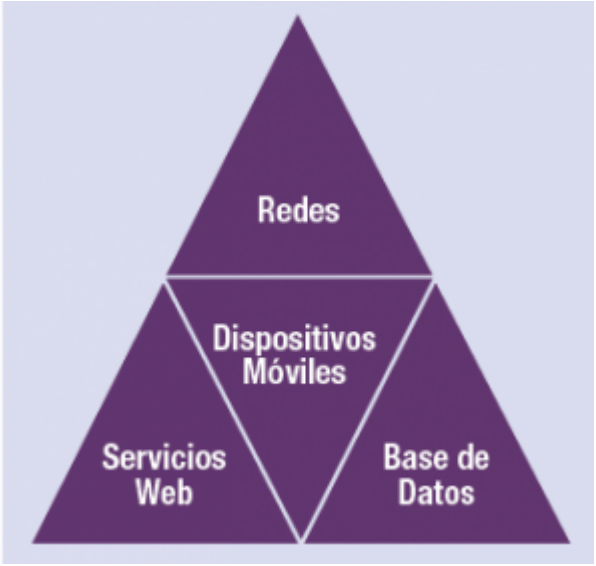
Policy, https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/policiesproceduresportablecomputingdevicesecurity (30/11/19)

Controles de auditoría en los pagos móviles

En el artículo anterior indicamos los riesgos que se producen al utilizar el dispositivo móvil para comprar por medio de internet. ¿Cómo podríamos prever esos riesgos? La respuesta se impondrá en este artículo en el cual se mostrará lo diferentes controles de auditoría que se deberán hacer.

Auditoria de pagos móviles

Para que la seguridad sea adecuada se dividen las diferentes partes que componen una aplicación de pagos móviles las cuales se muestran en la imagen[1]:



Cada uno de los componentes tienen sus controles y pruebas que se le hacen para prever la pérdida de la información, el acceso a persona no autorizadas y la pérdida de datos. En estas tablas se indica tanto donde se debe realizar el control como que tipo de prueba deberemos llevar a cabo.

Dispositivos móviles

Zona de riesgo	Prueba de control
Prever que cuando el dispositivo esté suspendido se evite la extracción de datos	¿El dispositivo móvil utiliza **AES**? Para prever la extracción de datos el dispositivo móvil debe estar configurado para realizar un cifrado avanzado **AES**(Advanced Encryption Standard).
La transmisión de datos debe estar cifrada	¿El cifrado se realiza mediante **SSL**(Secure Sockets Layer)? ¿Se usa **HTTPS** para el acceso a la web (Hypertext Transfer Protocol Secure)? ¿Se hace uso de **FTPS** (Comúnmente referido como FTP/SSL)para la transferencia de archivos? ¿Se usa **TLS**(Transport Layer Security)para los protocolos de seguridad?
La app limita el acceso la configuración apropiadamente	¿Se hace uso de un gestor de aplicaciones móviles **MAM**(Mobile Application Management) para administrar los accesos? Un ejemplo de **MAM** podrían ser **MobileIron**, **Airwatch**.

El código de la aplicación está protegido contra un intruso a través de protecciones binarias	¿La aplicación permite modificar el código? La aplicación debe estar configurar para limitar el acceso y la configuración adecuada para el uso limitado. Gestión de aplicaciones móviles **MAM** se utiliza para administrar acceso y despliegue de la aplicación.

Red

Zona de riesgo	Prueba de control
El cifrado del Wifi esta activada	¿La transmisión se realiza por medio de **SSL** o **TLS**(Transport Layer Security) para que la transmisión sea segura? La transmisión se realiza por medio de **SSL**(*Secure Sockets Layer*) o TLS(Transport Layer Security) ambos protocolos cifrados para que la transmisión sea segura.

Nombre del dominio sistema(DNS) realizando Spoofing. El DNS está protegido para evitar reencaminamiento de datos a otro Dirección de Protocolo de Internet (IP).	¿Se utiliza la **configuración adecuada** para el filtrado de paquetes? Se utiliza la configuración adecuada para el filtrado de paquetes utilizando **TLS**(Transport Layer Security), **SSH** y **HTTPS**(Hypertext Transfer Protocol Secure) debe estar habilitado,para, verificar la dirección de origen y bloquear paquetes con dirección conflictiva.
Perdida de datos de logueo debido a una conexión insegura.	¿Las conexiones de la **URL** son a través de **HTTPS**? Las conexiones de las **URL** (*Uniform Resource Locator*) a través de la **TLS** son a través de **HTTPS** en lugar de **HTTP** para asegurarse conectarse a una **URL**

Servidor web

Zona de riesgo	Prueba de control
Roles y responsabilidades para la propiedad ha sido establecida	¿Hay **diferentes** roles para los usuarios del servidor web? Los roles están correspondientemente definidos y cada uno de los roles con los accesos específicos.

Denegación de **DoS**(*Disk Operating System*) bloquear el acceso a los programas.	¿Se hace uso de **protocolos de bloqueo** y **captchas** para evitar ataques de **DoS** realizados por máquinas? Usar protocolos de bloqueo y **CAPTCHAS** para que diferencie máquinas de humanos.
Identificar y actualizar la aplicación para aumentar los parches de seguridad	¿Se ha encontrado una **vulnerabilidad nueva**? ¿Se ha generado la **actualización** para hacer frente a esta **vulnerabilidad**? Si se encuentra alguna nueva vulnerabilidad se debe gestionar un nuevo parche para solucionar esa falla de seguridad.

Base de datos

Zona de riesgo	Prueba de control
El acceso de alto nivel a las bases de datos	¿Los usuarios que tratan con la base de datos tiene **diferentes roles**? Asegurarse que tipo de acceso se tiene a la base de datos para cada persona. Todo esto se realizará por medio de cuentas y contraseñas

Consulta estructurada de la Base de datos	¿Se cumplen las **reglas de sintaxis** en la base de datos? Para cada tipo de sintaxis habrá unas reglas plenamente definidas con su respectiva valoración.
Los datos provenientes del móvil deben ser revisados antes de enviarlos a la base de datos	¿Los datos de la aplicación móviles están protegidos contra ataques mediante **verificaciones lógicas**? Los datos provenientes de la aplicación móvil deben estar protegidas a través de verificaciones lógicas dentro de la aplicación.

Gestor de aplicaciónes

Zona de riesgo	Prueba de control
El código fuente de la aplicación tiene correcto funcionamiento	¿La aplicación cuenta con la firma de la **empresa desarrolladora**? La aplicación utiliza el certificado de empresa desarrolladora además de su firma.
La información existe para mitigar el riesgo o la perdida de dispositivos comprometidos	¿Se hace uso de un **MAN** para facilitar la limpieza remota? Empleados de la empresa que hacen uso del control remoto de software de gestión móvil, como mobileIron para facilitar la limpieza remota

Las actuaciones de la tienda de aplicaciones so las correctas utilizando un ciclo de vida	¿La aplicación **específica** en la tienda la **actualización** que ha tenido y las **modificaciones** que se han realizado? Se le especifica a la tienda de aplicaciones las actualizaciones y modificaciones que se harán en la aplicación

En conclusión, los auditores TI deberán trabajar en la organización de responsables de la aplicación. Los auditores deben crear un **proceso de vigilancia** que determine un mínimo de **controles de seguridad** para que las aplicaciones puedan funcionar en una **zona con amenazas**. Además de este tipo de pruebas también se deberían hacer las **pruebas de penetración** cada vez que la aplicación móvil vaya a ser actualizada.

MobileIron

Es una empresa que se encarga de gestionar y administrar las aplicaciones para dispositivos inteligentes de forma segura y ahorrando costes. MobileIron hace uso de una plataforma virtual propia, donde se encuentran todas las aplicaciones móviles y se pueden descargar Mediante el uso de la plataforma se **reducen los errores** por ello se reducen los **costes económicos**, se aumenta la **productividad** y aumenta la **prevención de riesgos** [2].

Biografía

[1] “Journal volume 4 2016 spanish Issues https://www.isaca.org/Journal/archives/2016/volume-4/Documents/Journal-volume-4-2016-Spanish.pdf , (Consultado el 21/11/17).

[2] “MobileIron, aplicaciones para móviles en la nubehttp://empresayeconomia.republica.com/newsletter/mobileiron-aplicaciones-para-moviles-en-la-nube.html , (Consultado el 21/11/17).