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

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.
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.

Riesgos	Controles para uso recreativo	Controles para uso profesional
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.

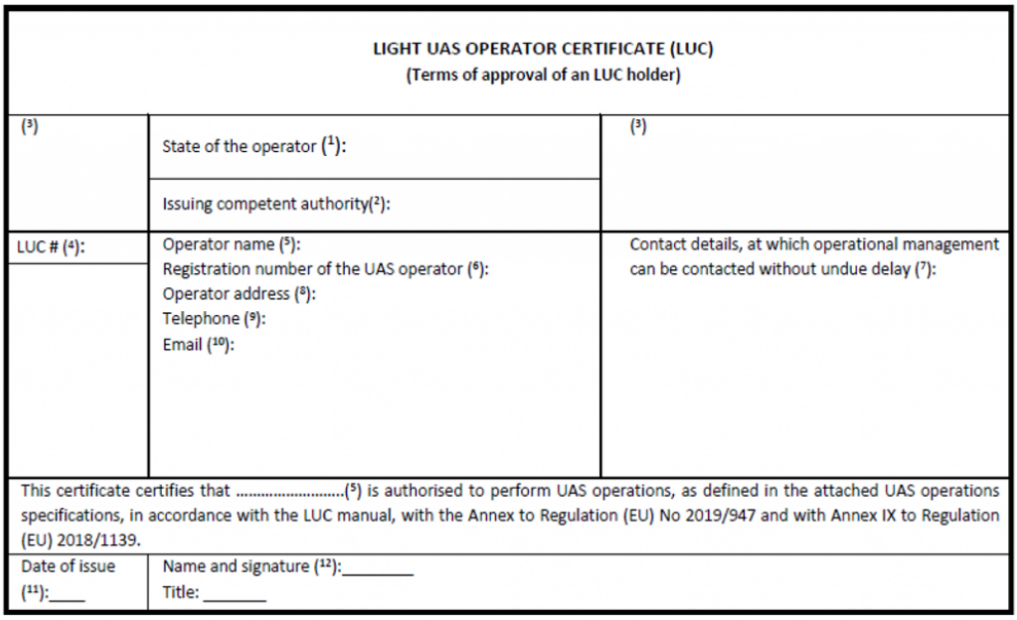
Riesgo	Controles
Ataque terrorista	• Vigilar visualmente el espacio aéreo cercano a zonas susceptibles de ser atacadas. • Rastrear la compra de drones por parte de posibles grupos terroristas.
Ataque de ciberseguridad	• Verificar la dificultad de robar físicamente los datos almacenados en el dron. • 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.

Riesgo	Controles
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.
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.

Cloud Computing, conclusiones

En este quinto y último post, me gustaría reflexionar sobre lo visto hasta ahora. Para ello, voy a destacar los **conceptos más relevantes de los cuatro posts anteriores** y os voy a traer una serie de opiniones y advertencias concretas que nos pueden dar mucho que pensar. En definitiva, me gustaría utilizar este post para ofrecer una **visión crítica** del Cloud Computing y **complementar los contenidos** que hemos ido viendo.

El Cloud Computing, como bien sabemos, es un **modelo para facilitar u ofrecer servicios y recursos de computación** (almacenamiento, procesamiento, gestión…) **bajo demanda, con elasticidad, escalabilidad y de forma remota** [1]. Un modelo opuesto a lo que conocemos como software on-premise.

Y recordado eso, reflexionemos, ¿por qué ha triunfado este modelo? ¿por qué se está adoptando de manera masiva por parte de las empresas? Podríamos pensar que es debido a los beneficios inmediatos que ofrece: escalabilidad, flexibilidad… Y es cierto, el Cloud Computing permite a las empresas ser más ágiles y reducir la complejidad de sus operaciones externalizando servicios y productos que no son su core de negocio [1]. Las empresas ya no tienen que desplegar infraestructuras TIC (**IaaS**, **PaaS**), y en ocasiones, ni siquiera deben desarrollar sus propias aplicaciones, pudiendo dedicarse a consumir software de terceros (**SaaS**). Además, los riesgos que tiene asociados este paradigma (ya sean técnicos o de gestión), como hemos podido ver, son controlables si contamos con un buen equipo de auditoría y un contrato blindado con el proveedor adecuado. Sin duda alguna, las ventajas que ofrece adoptarlo superan con creces a los inconvenientes.

Pero yo, como os decía al comienzo del post, os invito a verlo con otros ojos. Os invito a verlo con algo más de desconfianza. Si os fijáis, **el Cloud triunfa** no solo por lo que supone a nivel tecnológico o técnico, sino también **porque es mucho más barato que tener software on-premise** [1]. Al menos, de momento. Y esta última frase, pone sobre la mesa un riesgo que quizá no hayamos visto explícitamente en los posts anteriores. Y es probablemente, al menos a mi juicio, el más grave de todos.

Como vimos en el segundo post, hoy en día, el 94% de las empresas utilizan algún tipo de servicio Cloud. ¿Qué pasaría si de repente, visto que tantas empresas son dependientes del Cloud Computing, los proveedores comienzan a subir las tarifas? ¿Qué ocurriría si Amazon Web Services, Microsoft Azure o

Google Cloud se dan cuenta de lo necesarios que son para otras empresas y se aprovechan de la situación?

Pensaréis, bueno, si los proveedores suben los precios, las empresas volverán al modelo de software on-premise. Así que, tampoco pasaría nada. Al final, los proveedores tendrían que ceder. En mi opinión, eso no es así. No es tan sencillo.

Una vez se adopta el Cloud, los costes que supondría volver a traer de vuelta a casa los sistemas, plataformas e infraestructuras serían la **ruina de la mayoría de organizaciones**. Si hemos visto que es caro, complejo y difícil migrar de on-premise a Cloud. Pensadlo al revés, imaginad un **caso de repliegue**. Un caso en el que una empresa se vea forzada a volver al software on-premise, ya no por no haber realizado una migración adecuada al Cloud, sino porque no puede hacer frente a los compromisos económicos con el proveedor.

Vuelve a calcular tu plan de recuperación ante desastres (DRP) [2]. Vuelve a establecer un RTO y RPO. Vuelve a comprar el hardware. Vuelve a acondicionar las instalaciones oportunas. Vuelve a contratar técnicos de sistemas (y despide a tus especialistas en Cloud). Costes, costes y más costes inasumibles para muchos negocios.

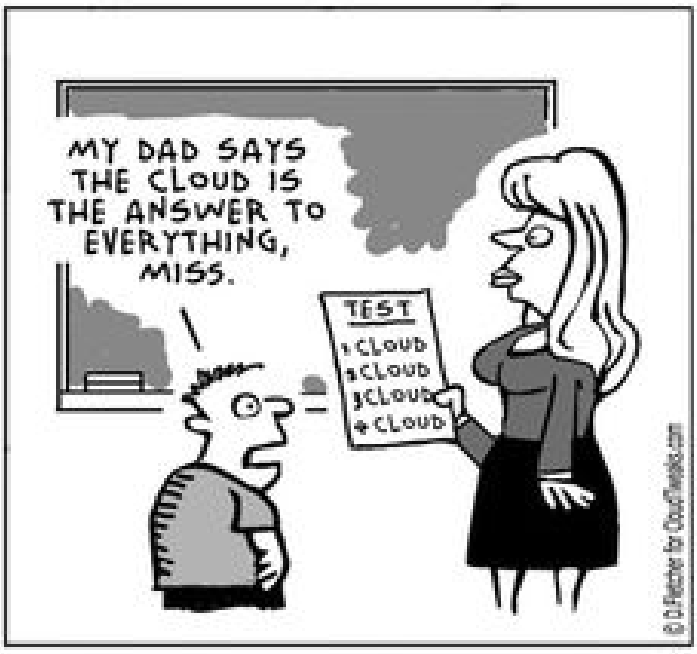
Decía Richard Stallman, un hombre sin duda polémico, que se equivoca con muchas cosas pero que acierta con muchas otras, que el Cloud Computing es una trampa elaborada para que las empresas compren sistemas cerrados y propietarios que les costarán cada vez más dinero [3]. Y si nos ponemos a pensarlo, debe ser un riesgo a considerar (más allá de lo que podamos opinar acerca del software privativo y el software libre). Al menos, yo así lo creo.

Debemos andar con pies de plomo cuando nos ponemos en manos de terceros. De hecho, ya vimos en el post de controles que **el Cloud Computing es puro Outsourcing**. En concreto, vimos que existe un control específico para (más o menos) lo que estamos hablando: “Asegurar que los procedimientos, capacidades y alternativas para migrar las operaciones en la nube a otro proveedor están previamente definidas al consumo del servicio en caso de que sea necesario por incumplimiento de los requisitos contractuales o cese del servicio del proveedor contratado”. Yo, personalmente, complementaria este control con la alternativa de volver al software on-premise. Y además, añadiría el riesgo de las **condiciones de renovación**, ya que igual no solo no encontramos otro proveedor, sino que igual procedemos a renovar contrato con el actual y nos encontramos con una subida de precios que no podemos asumir.

En relación a esto último, debemos saber que no solo existe el riesgo de no poder seguir pagando, ¡sino de pagar más de lo que creíamos que íbamos a pagar! ¿A qué me refiero con ésto? Pues que la propia elasticidad del Cloud supone un riesgo a la hora de predecir costes [2]. En otras palabras, añade complejidad y volatilidad a los presupuestos TI. De hecho, a veces acabamos pagando más de lo que pagaríamos con software on-premise [4].

Por otro lado, tal y como vimos en el post de riesgos y siguiendo esta línea de razonamiento pesimista, contratar software como servicio (SaaS) es una **pérdida de control total** para una organización [3]. En el futuro, veremos como empresas dependientes de proveedores SaaS se enzarzarán en batallas legales para poder seguir consumiendo servicios que han dejado de tener soporte, por acceder a datos históricos cuya existencia no estaba contemplada en el contrato o por defender que la propiedad intelectual de los resultados ofrecidos por el software les pertenece.

Con todo esto tampoco quiero dar a entender que el Cloud Computing es malo o que es peligroso. Nada más lejos de la realidad. Considero que **el Cloud Computing es el futuro**. Pero se suele decir que hasta que algo malo no pasa, no se toman medidas. Y en ese sentido, debemos ser críticos y, como auditores, anticiparse a la catástrofe, considerando tanto la esfera técnica como la de negocio cuando nuestra empresa quiera adoptar una nueva tecnología o un nuevo modo de hacer las cosas. Del mismo modo, no debemos caer en la trampa de que el Cloud es la solución a todos nuestros males. Quizá, nuestra organización no tenga la necesidad de adoptarlo, o incluso, no le convenga.



Asimismo, me gustaría aclarar que muchos de los problemas de los que hablamos

también existen, en cierto modo, en el modelo de software on-premise. Si compramos software, infraestructuras y plataformas para meter 'dentro de casa', su mantenimiento y renovación conlleva muchos riesgos [5]. Pero lo que es cierto, es que aquellos relativos a la **dependencia con terceros**, se magnifican con el Cloud Computing. En este post, como os habréis dado cuenta, he tratado de arrojar luz sobre dicho problema.

Además, me gustaría decir que la mayoría de los riesgos que hemos ido viendo (relativos a costes, control y privacidad) son mitigables, en parte, adoptando **modelos de despliegue de nube híbrida y privada**. Las diferencias de estos modelos con la nube pública ya las comentamos en anteriores posts. Principalmente, lo que se logra es reducir esa peligrosa dependencia con proveedores, manteniendo muchas de las ventajas del Cloud. Esto las empresas lo saben y es por ello por lo que está ocurriendo una migración masiva de nubes públicas a nubes híbridas y privadas [4]. Al principio resultan **más caras, pero a la larga, otorgan más control y seguridad**. Son la opción más prudente.

Finalmente deciros que, si os fijáis, da igual lo que estemos auditando, todo se reduce a identificar riesgos (tanto técnicos como de gestión), implantar controles, lanzarse a la piscina y, periódicamente, revisar que dichos controles se cumplen. Al final, si nos fijamos, la palabra auditoría, etimológicamente, viene del verbo latino audire. Esto es, viene del verbo oír. Un auditor lo primero que debe hacer es escuchar, ver, observar, para luego revisar, informar y recomendar.

Eso es lo que he tratado de hacer a lo largo de estos posts. Espero que os hayan servido para aprender sobre el Cloud y sobre todo, para aprender acerca del mundo de la auditoría TI. Para mí, ha sido un placer escribirlos. ¡Un saludo y gracias por leerme!

[1] «Computación en la nube – Beneficios, riesgos y recomendaciones para la seguridad de la información», ENISA, acceso el 28 de noviembre de 2019, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

[2] «How to escape the Cloud and move back to on-premise systems», TechRepublic, acceso el 28 de noviembre de 2019, https://www.techrepublic.com/article/how-to-escape-the-cloud/

[3] «Cloud Computing es peor que una estupidez», RedUsers, acceso el 28 de noviembre de 2019,

http://www.redusers.com/noticias/richard-stallman-cloud-computing-es-peor-que-una-estupidez/

[4] «Cloud Repatriation: When Is it Time to Bring Workloads Back On-Prem?», GreenHouseData, acceso el 28 de noviembre de 2019, https://www.greenhousedata.com/blog/cloud-repatriation-when-is-it-time-to-bring-workloads-back-on-prem

[5] «On Premise vs. Cloud: Key Differences, Benefits and Risks», Cleo, acceso el 28 de noviembre de 2019, https://www.cleo.com/blog/knowledge-base-on-premise-vs-cloud

---

Cuando se habla de salud, aceptar riesgos no es una opción

En el anterior artículo pudimos ver como los dispositivos médicos pueden manipularse para administrar dosis fatales de insulina, para robar datos de pacientes o incluso para directamente dejarlos inoperativos. Estos escenarios no son ciencia ficción. Son muy reales y cada vez son más los dispositivos médicos como marcapasos, bombas de insulina o máquinas de resonancia magnética vulnerables a sufrir ataques.

Mientras investigaba me he encontrado con un artículo [1] en el cual se recoge como varios investigadores emularon el funcionamiento de un dispositivo médico en un sistema de señuelo. En el transcurso de seis meses, los malhechores se conectaron con éxito en más de 55.000 ocasiones al sistema e instalaron más de 300 malwares. Esto refleja lo expuestos que estamos ante este tipo de ataques. Los dispositivos médicos están constantemente en peligro de ser comprometidos y es por ello que todo lo expresado hasta este post cobra especial relevancia.

Cuando hablamos de temas tan sensibles como es el caso de la salud de las personas, aceptar los riesgos no es una opción.

¿Y entonces qué hacemos?

Tenemos que gestionar dichos riesgos. La seguridad del paciente debería ser ante todo la prioridad de todos los fabricantes de dispositivos médicos.

Esta gestión, además, no resulta opcional sino que es un requisito reglamentario en todo el mundo. La FDA de los EE.UU. lo exige en el Reglamento del Sistema de Calidad. Europa, a su vez, lo requiere en el nuevo Reglamento de Dispositivos Médicos.

Asimismo, Japón, Canadá, Australia, Brasil y todos los demás mercados importantes también requieren la aplicación de la gestión de riesgos, a la cual se hace referencia en sus reglamentos nacionales o en la norma **ISO 13485:2016**. [2] Esta norma internacional respalda la obligación de los fabricantes de asegurarse de que los productos cumplen sistemáticamente los requisitos normativos aplicables y las exigencias del cliente. [3]

Sin embargo, todos ellos se rigen por la norma **ISO 14971**, norma mundial para la gestión de riesgos de los dispositivos médicos. Esta norma aprobada por la FDA, especifica el proceso de gestión de riesgos mediante el cual un fabricante puede identificar los peligros asociados con su dispositivo médico, estimar y evaluar los riesgos, **controlar** estos riesgos y supervisar la eficacia de los controles a lo largo del ciclo de vida del producto. [4]

Parece fácil, ¿verdad? No obstante, la realidad es que la gestión de riesgos es uno de los aspectos más complejos del cumplimiento de las regulaciones.

En este post, en concreto, nos vamos a centrar en los controles para mitigar los riesgos asociados a este tipo de dispositivos.

¿Pero qué es un control?

Un control es un proceso en cual se toman decisiones y se aplican medidas que permiten reducir los riesgos a niveles especificados.

Para cada uno de los riesgos es necesario estimar el **grado de impacto** así como la **probabilidad** de que este ocurra. A partir de estos valores se puede estimar si el riesgo resulta crítico, moderado o bajo pudiendo detectar aquellos riesgos sobre los cuales deberemos aplicar controles. [5]

¿Os acordáis de los riesgos que mencionamos en el anterior artículo?

Los hemos mencionado un poco antes: accesos no autorizados, ataques contra la disponibilidad, robo de datos, cambio de ajustes de configuración, software y firmware no probado o defectuoso …

Ahora vamos a intentar establecer una serie de controles para mitigar dichos riesgos: [6][7]

- **Establecer controles de acceso:** Consiste en limitar el acceso al dispositivo médico conectado a través de técnicas como la doble autenticación, uso de tecnologías NFC, establecimiento de contraseñas,… Este tipo de medidas permiten reducir el número de accesos no autorizados, reduciendo de esta forma también las posibilidades de sufrir un robo de datos. Sin embargo, este tipo de medidas pueden resultar polémicas en determinados casos: ¿Establecemos una contraseña de acceso en un marcapasos? De esto hablaremos un poco más adelante.
- **Realizar actualizaciones periódicas:** Es necesario aplicar parches de seguridad al dispositivo médico con frecuencia de acuerdo con las pautas posteriores a la comercialización emitidas por la FDA.
- **Aplicar estándares de codificación:** Muchos ciberataques exitosos han explotado vulnerabilidades presentes en el código que no han sido probadas rigurosamente antes de su implementación en un entorno activo. Una de las normas más importantes de la industria es la emitida por la Comisión Electrotécnica Internacional (IEC), IEC 62304. Este estándar proporciona una serie de características robustas sobre cómo desarrollar mejor el código.

- **Aplicar la seguridad mediante el diseño:** Es fundamental la gestión adecuada del ciclo de vida del dispositivo médico. Tener en cuenta la seguridad desde el primer momento en el cual se va a diseñar el dispositivo resulta fundamental.
- **Hacer uso de canales de comunicación cifrados:** Los dispositivos deberían hacer uso de canales de comunicación debidamente encriptados a fin de comunicarse con el mundo exterior.

Pero los controles no solo se deben establecer, estos a su vez deben ser **auditados**. Realizar auditorías periódicas de los procesos y de la tecnología ayuda a identificar las amenazas y permite mitigar los riesgos. Esta labor recae sobre los **auditores,** es decir las personas responsables de velar por la cumplimentación de las regulaciones correspondientes y de evaluar los procedimientos llevados a cabo por la organización.

Cuando se trata de auditorías de dispositivos médicos, las **pruebas de penetración** son un enfoque recomendado. Estas pruebas ayudan a evaluar lo fácil que es para los hackers violar la seguridad de los dispositivos para obtener recursos tales como datos, interrumpir operaciones o modificar sistemas que podrían afectar la salud del paciente.

Además, establecer controles no solo implica establecer iniciativas que solucionen el problema. Debemos ser conscientes también del ámbito en el cual se aplican. El otro día me enviaron una noticia en la cual el titular decía “Investigadores muestran la relación entre las brechas de datos y las tasas de mortalidad hospitalaria”. [8] Al principio pensé que la relación entre ambos factores sería las consecuencias generadas por el ataque. Sin embargo, la relación que establecía el estudio yacía en las contramedidas aplicadas por los hospitales y su consecuente aumento en los tiempos de atención a los pacientes.

Al final intentamos blindar los dispositivos y se nos olvida que en este sector en concreto se necesita de dispositivos seguros y efectivos pero que a su vez resulten rápidos en caso de emergencia. Imaginaros un médico que tuviera que estar introduciendo una contraseña mientras el paciente se está muriendo.

¿Y qué pasaría si al profesional sanitario se le ha olvidado la contraseña?

Somos humanos, estas cosas pueden pasar. Desde un punto de vista tecnológico esto supone un reto ya que cualquier mala implementación posee como resultado lo mencionado en el artículo, un aumento en la tasa de mortalidad.

Es por ello que se debe establecer una alineación entre las medidas aplicadas y el ámbito del mismo. ¿De que sirve blindar un dispositivo si en caso de emergencia no podemos acceder a él? ¿Tal vez tengamos que hacer uso de nuevas tecnologías? Y estas tecnologías a su vez, ¿ qué riesgos presentarían?

Muchas preguntas a contestar cuyas respuestas no resultan sencillas. Sin embargo lo que sí sé es que necesitamos dispositivos seguros, efectivos y alineados con el trabajo que realizan los profesionales del sector. En el momento en que se consiga alcanzar todo ello será cuando este sector alcance su máximo esplendor, pudiendo todos los ciudadanos aprovechar las ventajas que nos aporta la tecnología sin miedo a que nuestra vida corra peligro.

Y hasta que el post de hoy.

Referencias

[1] <<Closing the Gap in Medical Device Cybersecurity>>, Knowledge Leader, acceso el día 22 de noviembre del 2019, https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/hotissueclosingthegapinmedicaldevicecybersecurity

[2] <<ISO 14971 and the Basics of Medical Device Risk Management Explained>>, Oriel, acceso el día 22 de noviembre del 2019, https://www.orielstat.com/blog/iso-14971-basics-explained/

[3] <<ISO 13485 Certificación para los productos sanitarios>>, Lloyd’s register, acceso el día 23 de noviembre del 2019, https://www.lr.org/es-es/iso-13485/

[4] <<Case study – Risk management for medical devices (based on ISO 14971)>>, IEEE Xplore, acceso el día 20 de noviembre del 2019, https://ieeexplore.ieee.org/document/5754492

[5] <<The definitive guide to ISO 14971 risk management for medical devices>>, Green Light, acceso el día 22 de noviembre del 2019, https://www.greenlight.guru/blog/iso-14971-risk-management

[6] <<The Internet of Medical Things – Anticipating the Risk>>, ISACA, vol 4 (2019): 27-32

[7] <<Medical device cyber security guidance for industry>>, Australian Government, acceso el día 22 de noviembre del 2019, https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf

[8] <<Researchers Show Link Between Data Breaches and Hospital Mortality Rates>>, CPO Magazine, acceso el día 20 de noviembre del 2019, https://www.cpomagazine.com/cyber-security/researchers-show-link-between-data-breaches-and-hospital-mortality-rates/?mc_cid=61cc16581e&mc_eid=5a73407028

Cloud Computing, controles

En el post anterior recorrimos las **diferentes tipos de riesgos** que presenta el Cloud Computing y terminamos diciendo que es **necesario utilizar los controles adecuados** para poder mitigarlos. Y estos controles, comentamos que los íbamos a encontrar en **marcos de trabajo**. Pues bien, dedicaremos este post a explicar lo que son los controles y qué debe hacer un auditor para asegurarlos. Asimismo, y a modo de ejemplo, estudiaremos una serie de controles que responden a riesgos concretos que he extraído de diferentes fuentes. Sin más dilación, comenzamos.

¿Qué es un control? En pocas palabras, podríamos decir que es un **mecanismo que define una organización con la finalidad de mitigar un riesgo**. Y con mitigar nos referimos a, por un lado, reducir la probabilidad de ocurrencia del riesgo y, por otro lado, reducir el daño que pueda causar en caso de que ocurra. Estos criterios, **probabilidad e impacto**, aunque no lo dijéramos en el anterior post explícitamente, suelen ser los dos ejes de análisis a la hora de priorizar los riesgos.

Para entenderlo mejor, pongamos un ejemplo. Si tenemos un riesgo concreto de privacidad y seguridad (tal y como vimos en el anterior post) con los datos que almacenamos en la nube, póngase, riesgo de que nuestros datos sean interceptados por terceros no autorizados en la red de comunicaciones que mantenemos con el proveedor, podríamos tener el siguiente control: asegurar que los datos en tránsito por las redes de comunicación oportunas entre

proveedor y consumidor están encriptados con claves privadas que solo conoce el segundo [1]. Esto es, si cumplimos con lo que dice el control, logramos mitigar el riesgo.

¿Fácil? Pues en realidad es más complejo de lo que parece. En primer lugar, existen multitud de riesgos concretos que debemos tener en cuenta, y es por eso, que como decíamos en el anterior post, vamos a necesitar guías y marcos de trabajo que nos permitan considerarlos sin que se nos escape ninguno. Y además, y esto aún no lo he dicho, **los controles no solo deben implementarse… Deben auditarse**. En otras palabras, debe asegurarse que los controles se cumplen. Y para ello, lo normal es que cuando se define un control, se le asocien una serie de pruebas de control o acciones de auditoría.

Para ese mismo ejemplo que veíamos antes, recogido de un documento oficial de ISACA [1], se definen las siguientes acciones de auditoría: (1) obtener las políticas de encriptación y procedimientos para datos en tránsito de la organización, (2) evaluar si los procedimientos incluyen lo siguiente: clasificación de datos en función de la sensibilidad (top secret, confidential, company confidential, public), tecnologías de encriptación adecuadas, gestión de claves apropiada y una lista de organizaciones externas del consumidor que poseen las claves de desencriptado. ¿Ya es algo más concreto verdad? Parece que empezamos a tener el control, valga la redundancia, sobre el control que hemos definido para el riesgo que queremos mitigar.

Dicho esto, y ahora que entendemos lo que es un control y cómo se debe asegurar, he tratado de identificar ciertos riesgos concretos para nuestro paradigma, el Cloud Computing, con el objetivo de haceros ver algunos controles que nos pueden ayudar a mitigarlos. Con esa finalidad, he construido una **tabla con tres columnas**: dominio (tipo de área donde se enmarca el control), control (definición del control, lo que se debe hacer) y riesgo mitigado (problema al que responde el control).

Para construir dicha tabla, me he apoyado principalmente en el documento [1], el cual define una serie de controles para la mitigación de riesgos en el Cloud Computing haciendo uso del marco de trabajo **COBIT** y el marco de trabajo **COSO ERM**. Mi trabajo ha consistido en agrupar los controles más significativos, descartar aquellos redundantes, resumirlos, clasificarlos por dominios y relacionarlos con el riesgo que buscan mitigar. Además, he usado a modo complementario los documentos [2] [3] [4] y he considerado los contenidos del anterior post para la definición de los riesgos mitigados. La tabla es la siguiente:

Dominio	Control	Riesgo mitigado
Gestión de identidades y accesos.	**Asegurar** una **asignación y designación de identidades** en las aplicaciones alojadas en la nube de la organización **controlada y alineada con las políticas internas** de gestión de usuarios.	Acceso no autorizado a recursos y datos.
	Asegurar que la **responsabilidad de la autenticación de usuarios pertenece al consumidor** del servicio y que se usan **tecnologías single sign-on y OpenID** para todos los servicios consumidos.	Acceso no autorizado a recursos y datos.
Seguridad e integridad de datos.	**Encriptar los datos en tránsito** por las redes de comunicación oportunas entre proveedor y consumidor con claves privadas que solo conoce el segundo. Uso de una **VPN** apropiada.	Revelación y pérdida de datos.
	Encriptar los datos contenidos en las bases de datos y sistemas del proveedor con claves que solo conozca el consumidor.	Revelación y pérdida de datos.
	Encriptar los datos de las copias de seguridad de las bases de datos y sistemas del proveedor.	Revelación y pérdida de datos.
	Confirmar que los **datos de prueba (testing) no contienen información confidencial o sensible**, y que no se usan datos históricos del sistema de producción para testear aplicaciones alojadas en la nube.	Revelación de datos.
	Asegurar que las **claves de encriptado** están **protegidas adecuadamente** ante accesos no autorizados, que existe una **segregación de deberes** entre los gestores de las claves y los usuarios a través de una **política de gestión de claves** y que las claves tienen **copias de seguridad**.	Revelación y pérdida de datos.
Portabilidad e interoperabilidad.	**Asegurar** que los **procedimientos**, **capacidades** y **alternativas** para **migrar las operaciones en la nube a otro proveedor están** previamente **definidas** al consumo del servicio en caso de que sea necesario por incumplimiento de los requisitos contractuales o cese del servicio del proveedor contratado.	Impacto en la continuidad de negocio. Interrupción de los servicios prestados.
Seguridad de sistemas e infraestructuras.	**Asegurar** que los **sistemas** están **aislados y protegidos** por controles de seguridad a través de **herramientas de virtualización** para prevenir accesos no autorizados y ataques.	Indisponibilidad de sistemas y revelación de datos.

	Confirmar que el **diseño** de las aplicaciones alojadas en la nube incluye **aspectos de seguridad a nivel de arquitectura** aprobados por expertos y que dicho diseño hace hincapié en las **interdependencias con otros sistemas** y aplicaciones.	Indisponibilidad de sistemas.
	Confirmar que todas las **herramientas** utilizadas en el **desarrollo, gestión y monitorización** de las aplicaciones están **documentadas, aprobadas y analizadas** en función del efecto que puedan causar en los controles de seguridad establecidos.	Indisponibilidad de sistemas y revelación de datos.
Contratos.	**Asegurar** que el **equipo legal del consumidor ha identificado y comunicado** al proveedor los **requisitos contractuales** oportunos, y que este último, ha aceptado cumplirlos.	Incumplimiento de obligaciones contractuales.
	Confirmar que el **consumidor realiza una monitorización** constante para confirmar que **se cumplen** las **obligaciones reflejadas en el contrato** con el proveedor.	Incumplimiento de obligaciones contractuales.
Cumplimiento.	**Asegurar** que los aspectos legales relativos a **requisitos funcionales, jurisdiccionales o contractuales son considerados por ambas partes**, **proveedor** y **consumidor**, estando todos ellos documentados, aprobados y monitorizados.	Incumplimiento normativo.
	Confirmar que todas las **regulaciones** sobre **protección de datos** que afectan a las actividades de la compañía están **identificadas, clasificadas y documentadas**. **Asegurar** que la **plataforma** de Cloud Computing contratada **no incumple ninguno de los requisitos u obligaciones** contempladas en dichas regulaciones.	Incumplimiento normativo.
	Asegurar que las **responsabilidades de protección de datos están correctamente definidas y repartidas** entre proveedor y consumidor en función del modelo de despliegue elegido.	Incumplimiento normativo.
	Asegurar que el **proveedor** ofrece garantías de seguridad a través de la **certificación ISO 27001**.	Incumplimiento normativo.

Tabla. Controles y riesgos mitigados Cloud Computing.

Espero que esta tabla os haya servido para haceros una idea de qué controles necesitamos si nuestra compañía quiere adoptar el Cloud. Supongo que os habréis dado cuenta, que tal y como adelantamos en el anterior post, todo gira entorno a controlar la **complejidad del paradigma** y asegurar que trabajamos con un **tercero que** nos **ofrece** las **garantías** necesarias. Asimismo, comentaros que si os quedáis con la curiosidad y queréis ver qué acciones de auditoría concretas tiene asociadas cada control, os recomiendo acudir al documento [1].

Para finalizar, como reflexión, permitidme deciros que si os fijáis, existen muchos tipos de controles, algunos más técnicos y otros quizás más de gestión. Y que a veces, al menos yo (como estudiante de ingeniería) y con ciertas preferencias personales hacia el mundo del desarrollo, nos cegamos con los aspectos tecnológicos y no somos capaces de ver lo importantes que son los aspectos organizativos. Si no hay una política de gestión de claves bien definida, da igual lo sofisticado o puntero que sea tu sistema criptológico, vas a tener vulnerabilidades. De la misma manera, por muy buena política de gestión de usuarios que hayas definido, como no uses una tecnología robusta que permita implementar de manera segura sus directrices, tienes un problema. Lo mismo, para los contratos y cumplimientos…

Con esto simplemente os quiero hacer ver que las TIC deben estar alineadas con negocio. Que las TIC, cada vez están más afianzadas como parte de la estrategia de la organización. Y que las TIC, cada vez están más lejos de ser una simple capa de soporte. En definitiva, quería remarcar que un **auditor TI** no es solo un profesional que asegura con su buen criterio que todo está en orden, sino también un **puente entre** el **negocio** y la **tecnología**.

Hasta aquí el cuarto post. ¡Gracias por leerme y nos vemos en el siguiente!

[1] «IT Control Objectives for Cloud Computing», ISACA, acceso el 16 de noviembre de 2019, https://www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20contro%20objectives%20for%20Cloud%20computing.pdf

[2] «Protiviti’s View on Emerging Risks – Cloud Computing», KnowledgeLeader, acceso el 16 de noviembre de 2019, https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/nlpreviewjuly2019

[3] Zacharias Enslin, «Cloud computing adoption: Control objectives for information and related technology (COBIT) – mapped risks and risk mitigating controls». African Journal of Business Management 6 37 (2012): 10185-10194, acceso el 16 de noviembre de 2019, https://oceano.biblioteca.deusto.es/permalink/f/193pu0n/TN_crossref10.5897/AJBM12.679, https://academicjournals.org/journal/AJBM/article-full-text-pdf/363FCF530555

[4] «Riesgos y amenazas en Cloud Computing», INTECO-CERT, acceso el 16 de noviembre de 2019, https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf