Buena cautela, iguala buen consejo

En el post anterior hablé sobre los riesgos que entrañaba usar un dron comercial, y aunque haya muchos más, ya es hora de ponernos en el rol del auditor y establecer unos controles que deberían de llevarse a cabo. Los riesgos los habíamos dividido en dos partes, los intencionados por las personas y las que no lo son, por lo que los controles irán también divididos en los mismos grupos para confeccionar nuestra matriz de riesgo y controles.

Entre los riesgos intencionados, relacionados [1] con las personas y las oportunidades que ofrecen los drones, se pueden identificar varios controles relacionados con la seguridad informática, la privacidad y mecanismos de emergencia como último recurso.

Para verlo en sintonía con los riesgos, la siguiente tabla [2] explica con mejor detalle la relación entre los riesgos y los respectivos controles que deberían cumplirse para evitarlos, aceptarlos o minimizar impactos.

Riesgo	**Impacto en el negocio**	**Descripción de medidas**	**Controles**
Robo de datos	Pérdida de privacidad de la gente, desconfianza como proveedor de servicios, filtrado de información sensible de infraestructuras o credenciales.	Hacer uso de canales seguros a la hora de enviar información y evitar el acceso simultáneo de usuarios al dron.	1. Cifrado de los datos de punto a punto. 2. Utilizar protocolos seguros a la hora de la comunicación. 3. Control de accesos.
Secuestro del dron	Pérdida de un activo, retraso en el trabajo y perder tiempo y dinero en los procesos de investigación del incidente	Conseguir una manera de evitar el secuestro [3], activando protocolos de rescate para aterrizar al dron o reforzando la seguridad tanto en el programa como en los protocolos y frecuencias de comunicación usadas.	1. Control de acceso. 2. Implementar protocolos de rescate. 3. Instrucción a los pilotos sobre los peligros 4. Uso de frecuencias seguras.

Secuestro y destrucción del dron	Pérdida doble, por una parte el dron, y por la otra el objetivo del perpetrador, daños al negocio y a terceros.	Además de lo del riesgo anterior, evitar el impacto, implementar programas de evasión de choques y no poder evitarlos.	1. Implementar medidas evasivas. 2. Asegurar la integridad del software de evasión 3. Control de acceso. 4. Implementar protocolos de rescate. 5. Uso de frecuencias seguras. 6. Instrucción a los pilotos sobre los peligros.

Algunos controles se comparten debido a que los riesgos intencionados más importantes están centrados en la seguridad. Aunque los controles de robo de datos se establezcan [4], las tecnologías utilizadas para el hacking siguen creciendo, por lo que los controles planteados servirían para intentar mitigar los ataques ya conocidos. Hasta los drones se pueden usar para hackear otros drones, lo que conlleva a fortalecer las medidas de seguridad de manera enorme.

Para los riesgos no intencionados, los controles necesarios están más centrados en la decisión de pilotar y evitar el máximo los daños del entorno como del dron. En la siguiente tabla, siguiendo el modelo de la anterior se reflejan unas medidas de mitigar los riesgos generalmente debido a la naturaleza de los mismos.

Aunque se implementen ciertos controles como para reducir o mitigar los desastres que pueden ocurrir, cada empresa que haga uso de los drones tendrá unos riesgos y unos controles diferentes para aplicar, por lo que no es fácil determinar un guión general. En el siguiente post, entraré con más detalle sobre si la empresa que posees tiene la imperiosa necesidad de usar drones, le ayudaría en el negocio debido a las ventajas sobre los riesgos que podría suponer o si simplemente tenerlos es un capricho.

Bibliografía:

[1]«PreView Volume 3, Issue 2», Protiviti, acceso el 21 de noviembre de 2019, https://www.protiviti.com/US-en/insights/preview-vol-3-issue-2

[2]«Trading skills & essentials,risk management», Investopedia, acceso el 23 de noviembre de 2019, https://www.investopedia.com/terms/r/risk-control.asp

[3]«Así se puede hackear un dron en pleno vuelo», As-Betech, acceso el 26 de noviembre de 2019, https://as.com/meristation/2016/10/28/betech/1477685427_331526.html

[4]«Rise of the Drones», ISACA emerging tech report, acceso el 24 de noviembre de 2019,

http://www.isaca.org/Knowledge-Center/Research/Documents/Rise-of-the-Drones_whp_eng_0217.pdf