Controles y auditoría en el mundo de los drones

Hoy vuelvo con una entrada más en la serie de posts sobre drones. En el post anterior realicé un análisis de los riesgos que conlleva el uso de los drones en diferentes situaciones. En esta ocasión, completaré dicho análisis mediante la definición de los controles necesarios para mitigar cada uno de los riesgos identificados. Por otro lado, destacaré el rol del auditor en el contexto de los drones.

Los controles son un elemento clave en el mundo de la auditoría. Son el conjunto de procedimientos que tienen como objetivo reducir la probabilidad de ocurrencia de un determinado riesgo, o minimizar la severidad del daño que dicho riesgo pueda causar (concretamente los dos criterios utilizados en el post anterior para establecer el nivel de importancia de cada riesgo). Generalmente, estos procedimientos o controles suelen estar basados en estándares y marcos de trabajo internacionales que se consideran buenas prácticas y que aseguran que todos los aspectos relevantes que deben incluir los controles han sido considerados. A continuación muestro la lista de riesgos identificados en el post anterior (agrupados en **riesgos intencionados** y **riesgos no intencionados**), acompañados de los **controles** específicos que deberían realizarse para mitigar cada uno de los riesgos:

Riesgos intencionados

Riesgo	Nivel de riesgo	Controles

Atentado terrorista	Alto	• Establecer perímetros de seguridad sobre los espacios de máximo riesgo. • Identificar puntos ciegos de visibilidad y asignar equipos de seguridad. • Desplegar controles de seguridad en los accesos a los recintos.
Espionaje	Medio	• Verificar que la totalidad del área restringida se encuentra bajo vigilancia ininterrumpida, incluyendo los espacios aéreos. • Asignar equipos de actuación frente a la detección de una intrusión.
Violación de privacidad	Alto	• Identificar áreas de gran visibilidad y ocultarlas al salir de la vivienda. • No dejar a la vista información sensible como números de cuenta bancaria o contraseñas.
Robo de datos	Alto	• Verificar que la información almacenada en el dron se encuentra cifrada mediante un algoritmo de cifrado robusto. • Utilizar claves de descifrado largas y complejas. • Utilizar conexiones cifradas para la comunicación con el dron. • Acorazar el dron para impedir el acceso a los dispositivos de almacenamiento de datos.

Riesgos no intencionados

Riesgo	Nivel de riesgo	Controles

Colisiones contra aeronaves	Alto	• Consultar las cartas aeronáuticas de la OACI para conocer las zonas de vuelo y sus restricciones[1]. • Verificar que se vuela a una distancia mínima de 8 km de cualquier aeropuerto o aeródromo. • Volar de día, con buenas condiciones meteorológicas y no superando los 120 metros de altitud de vuelo[2].
Colisiones contra estructuras terrestres	Medio	• Verificar que se vuela lejos de cualquier entorno urbano. • En el caso de hacer un uso profesional, verificar que se cuenta con el título de piloto de drones y estar dado de alta como operador en la AESA. • Verificar que el dron se encuentra en todo momento dentro del alcance visual del piloto.
Colisiones contra personas	Alto	• Verificar que no se vuela cerca de aglomeraciones de personas. • Verificar que se vuela lejos de cualquier entorno urbano. • Volar de día, con buenas condiciones meteorológicas y dentro del alcance visual del piloto.

Colisiones contra aves	Alto	• Si se vuela en un espacio natural protegido, verificar sus restricciones de vuelo. • Volar de día y en buenas condiciones meteorológicas. • Mantenerse alejado de las bandadas de aves.
Interferencias	Medio	• Consultar las cartas aeronáuticas de la OACI para conocer las zonas de vuelo y sus restricciones. • Verificar que se vuela a una distancia mínima de 8 km de cualquier aeropuerto o aeródromo. • Utilizar bandas libres para la comunicación con el dron.
Actividad crítica fallida	Alto	• Verificar que el nivel de batería del dron es el máximo antes de comenzar la actividad. • Realizar revisiones regulares del estado de las piezas principales del dron. • Comprobar funcionamiento correcto del dron antes de comenzar la actividad.

Al tiempo en que nuevas tecnologías entran en el mercado, los auditores se ven obligados a expandir sus conocimientos y adaptarse a estas innovaciones. El caso de los drones no es una excepción. Los drones son una tecnología muy reciente (al menos en el contexto comercial), por lo que en ocasiones no implementan las medidas de seguridad adecuadas, dejando vulnerabilidades que pueden comprometer seriamente a las organizaciones o instituciones que hacen uso de estos aparatos. Es ahí donde entra en juego el papel del auditor, como es el caso de la auditoría que recientemente se ha

realizado al Departamento de Seguridad Nacional de los Estados Unidos por causa del uso de drones para patrullar la frontera entre México y Estados Unidos. El informe resultante de dicha auditoría declara que los sistemas de información utilizados por la Oficina de Aduanas y Protección Fronteriza de los Estados Unidos para la compartición de datos recogidos por los drones, presentan riesgos de seguridad de la información, tanto por orígenes internos como externos. El informe detalla que las causas de dicho riesgo son la falta de monitorización de los sistemas, falta de gestión de incidentes, falta de personal suficiente, desactualización de sistemas operativos e incluso políticas de seguridad inefectivas, ya que se registraron más de 20 accesos de dispositivos extraíbles no autorizados en los sistemas[3].

Con casos como este podemos concluir que cada vez es más importante el rol de la auditoría en las nuevas tecnologías, como pueden ser los drones, que son capaces de almacenar información comprometida, por lo que es indispensable efectuar los controles necesarios.

Referencias:

[1] Gis&Beers, <<Legislación internacional sobre drones>>, 25 de junio de 2017, acceso el 25 de noviembre de 2018, http://www.gisandbeers.com/legislacion-internacional-drones/

[2] Aerial Insights, <<Normativa sobre drones en España>>, octubre de 2018, acceso el 25 de noviembre de 2018, http://www.aerial-insights.co/blog/normativa-drones-espana/

[3] Sean Lyngaas, <<DHS drone data left vulnerable, audit

finds>>, *Cyberscoop*, 25 de septiembre de 2018, acceso el 25 de noviembre de 2018, https://www.cyberscoop.com/dhs-drone-data-left-vulnerable-audit-finds/