Si ciertos datos cayesen en manos del adversario y se atentase contra su confidencialidad, podríamos tener consecuencias con un elevado impacto en una operación militar

Daniel Benavente López. Ingeniero de Telecomunicación.
Ingeniero de Sistemas. Coordinador Área de Ciberdefensa de Isdefe.
Prestando servicio al Mando Conjunto del Ciberespacio.

Ciberdefensa, seguridad y control de la información

La seguridad de las tecnologías de la información y la comunicación es un área extremadamente amplia, con diferentes enfoques y una gran trayectoria desarrollada durante muchos años. En este artículo se aborda una de sus aproximaciones, la que se centra en la seguridad del dato, desde la perspectiva del Mando Conjunto del Ciberespacio (MCCE) de las Fuerzas Armadas, que trata de aunar la seguridad de los sistemas con la ciberdefensa para conseguirlo.

Antes de que el término 'ciberseguridad' estuviese tan extendido, o de que se hablase ampliamente sobre 'ciberdefensa' (sobre todo en el entorno militar, con el primer Concepto de Ciberdefensa del JEMAD del año 2011) o sobre el 'ciberespacio' (reconocido como dominio de operaciones en la OTAN hace relativamente poco tiempo, en 2016), uno de los acrónimos más utilizados en el Ministerio de Defensa era STIC, es decir: Seguridad de las Tecnologías de la Información y la Comunicación.

Tanto las Administraciones Públicas como las entidades privadas han trabajado y vivido su evolución a lo largo del tiempo. Quizás, muchos años atrás, se concebía como algo más secundario, pero fue cobrando importancia hasta convertirse en algo primordial y prioritario para la mayoría de las organizaciones, dado el elevado impacto potencial asociado la materialización de amenazas en los sistemas. Estas son capaces de provocar consecuencias de muy diversa índole, que pueden ir desde la pérdida económica o de reputación, hasta incluso poner en peligro la vida de las personas.

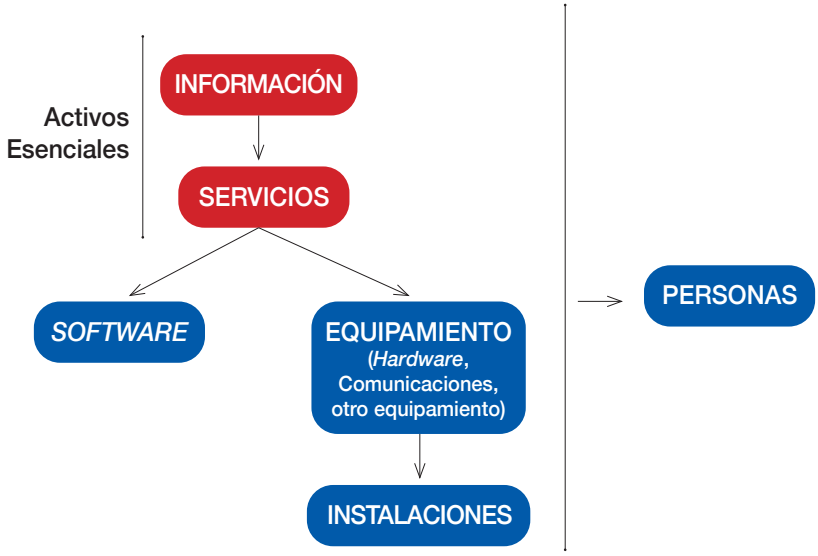
Cómo abordamos la seguridad en los sistemas

Una de las aproximaciones más aceptadas es la que se enfoca no solo en los propios sistemas, sino que toma como base la información que se maneja en ellos, un enfoque centrado en la seguridad del dato. Esta estrategia es la que pretende abordar la Seguridad de la Información en los Sistemas de Información y Telecomunicaciones o, como se conoce en el Ministerio de Defensa, SEGINFOSIT.

Pero, ¿por qué proteger estos sistemas sobre la base de los datos que manejan? Desde tiempos inmemoriales, la información se ha considerado como un activo tremendamente valioso que puede otorgar una gran ventaja a quien

Figura 1. Esquema de dependencias para análisis de riesgos en MAGERIT.

Fuente propia. Transcripción de Figura de la Guía de Seguridad de las TIC CCN-STIC 470 PILAR – Manual de Usuario v7.1



ostente su control (recordemos esa famosa frase: "la información es poder"). A pesar de que los sistemas tienen su propio valor, los datos que albergan y que manejan o envían (almacenados, en procesamiento o en tránsito), se erigen como uno de los activos más relevantes que es necesario proteger.

Veámoslo desde una perspectiva de análisis y gestión del riesgo, y tomemos como base una metodología clásica formal, como MAGERIT. El esquema de dependencia de activos recomendado por el Centro Criptológico Nacional en sus guías pone en la cúspide de la pirámide a los datos. La información y los servicios que corren por estos sistemas se denominan 'activos esenciales'. Son ellos los que van a dar un valor acumulado (heredado) a los sistemas (*software* y equipamiento) que será necesario proteger, no tanto por su valor propio sino por el que les otorgan esos los activos esenciales mediante las dependencias.

Por qué nos centramos en la información

Pero, ¿de verdad la información es tan relevante como para adoptar un enfoque de seguridad basado en ella? Imaginemos por un momento información clasificada corriendo por Sistemas de Mando y Control Militar que dan soporte a una operación. En el caso de que ciertos datos cayesen en manos del adversario y se atentase contra su confidencialidad, podríamos tener consecuencias con un elevado impacto en una operación militar, e incluso en la seguridad de las personas que están sobre una zona de operaciones. No hemos de ir muy lejos para trasladar este ejemplo a un conflicto armado actual, extrapolando el peligro que supondría, por ejemplo, la revelación de la posición de nuestras tropas al enemigo.

Imaginemos ahora que estos datos además son modificados sin conocimiento ni consentimiento de las personas que están trabajando con ella, y lo hacen con una base errónea. ¿Y si no podemos acceder a la información o a los servicios en el tiempo y forma adecuados? Igualmente, ambos supuestos podrían tener graves consecuencias en el curso de una operación militar.

De estos tres ejemplos podemos deducir la importancia de proteger la confidencialidad, la integridad y la disponibilidad de la información. Si alguna de estas dimensiones es afectada, podría tener impactos negativos. De ahí que la protección del dato sea una prioridad.

Un poco de historia

Desde hace muchos años, en el Ministerio de Defensa se ha tratado de proteger los sistemas con la orientación de salvaguardar los datos que se manejan en ellos. Si nos remontamos al año 2002, se desarrolló la Política de Protección de la Información del Ministerio de Defensa almacenada, procesada o transmitida por Sistemas de Información y Telecomunicaciones. En aquellos tiempos, un término muy extendido era el de INFOSEC, altamente utilizado en OTAN.

La protección más clásica se centraba en asegurar lo mejor posible las dimensiones de seguridad de confidencialidad, integridad y disponibilidad. Posteriormente fue evolucionando y se abarcaron otras dos: la autenticidad ("una entidad es quien dice ser y/o se garantiza la fuente de la que proceden los datos", según la definición del Esquema Nacional de Seguridad) y la trazabilidad ("las actuaciones de una entidad pueden ser trazadas de forma indiscutible hasta dicha entidad").

En el Ministerio de Defensa, la SEGINFOSIT, dirigida actualmente por el comandante del Mando Conjunto del Ciberespacio, se orienta a proteger los sistemas para salvaguardar la información que estos manejan, con el objeto de garantizar razonablemente la confi-

La Seguridad de la Información en los Sistemas de Información y Telecomunicaciones se conoce como SEGINFOSIT en el Ministerio de Defensa