LA "GUERRA DE GILA" Y LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

¿Imaginan ustedes qué pasaría si cada vez que se produce el relevo del comandante de un barco de la Armada Española tuviéramos que "empezar desde el principio"?

Permítanme que les explique, soy oficial de la Armada, aunque desde hace ya unos cuantos años haya cambiado la cubierta de los barcos por la seguridad de la información. Esta actividad, en la que desarrollo mi trabajo diario para el Ministerio de Defensa, me parece fascinante y llena de retos y exigencias, aunque no consiga hacerme olvidar la época en la que estuve a bordo de distintos buques. Por ello, y para ayudarme a sobrellevar mi añoranza, he querido plantearles la pregunta con la que he empezado este artículo.

Imaginen qué pasaría si cada vez que se produce un relevo en el mando de un buque hubiera que acordar quién es el enemigo, cuál es el origen de las crisis y de los conflictos, qué es lo que hay que defender y quiénes son los aliados. Quizás, también habría que determinar si es más probable que el enemigo venga del sur o del norte, y si es más importante defender la costa que la flota mercante que se encuentra navegando.

¿Y qué sucedería con sus medios de defensa? ¿Debería ser el comandante el que decidiera si la formación de la dotación es estratégica para alcanzar niveles satisfactorios de autodefensa? ¿o si se deben realizar inspecciones por personal externo al buque para evaluar si los procedimientos se aplican correctamente?

Pues aún hay más, el cambio del comandante de un buque se produce cada año y medio aproximadamente. ¿Imaginan las consecuencias? ¿Recuerdan al inolvidable humorista Gila, armado con su casco y su teléfono, y haciendo parodias sobre la guerra? No sufran, pueden estar tranquilos, un buque de guerra es un entorno mucho más serio y formal que el que les acabo de describir. En un barco todo está "atado y bien atado", y el relevo entre comandantes no afecta a su misión, objetivos y funcionamiento.

Norma de normas

Pero, ¿qué ocurre con la seguridad de la información en las organizaciones? ¿se improvisa o se actúa como un buque de guerra?

Generalmente, y a diferencia de lo que sucede en los barcos, en el mundo de la seguridad no siempre hay políticas y procedimientos escritos. A veces no se cuenta con apoyo suficiente de la dirección, que no es consciente del peligro que supone aplicar la "*Guerra de Gila*" a la gestión de la seguridad de la información. En otras ocasiones, los que trabajamos en seguridad de la información somos reacios a "izar velas" y ponernos a redactar normativa, quizás por tener un perfil demasiado "tecnólogo".

La política de seguridad de la información puede verse desde una doble perspectiva. Por un lado se puede considerar como la norma de normas, la "constitución" de la seguridad de la información, en la que se recogen principios esenciales, comúnmente aceptados por toda la organización, que inspiran su comportamiento y que, aunque no sean inamovibles, perduran en el tiempo. Por otro, podemos considerar la política de seguridad de la organización como el cuerpo normativo de seguridad que comprende a la propia política y al resto de las normas, procedimientos y guías. De esta manera, y cuando nos referimos a la necesidad de que un empleado conozca y cumpla la política, estamos utilizando esta segunda aproximación.

> Una buena política de seguridad de la información debe estar muy centrada en el negocio y en los requisitos específicos de cada organización y, por tanto, no sirven soluciones "estándar" que se reutilizan una y otra vez.

Sin embargo, quisiera centrarme en la primera acepción, por ser la política el pilar esencial en el que se debe basar el diseño y la construcción del modelo de seguridad de cualquier organización. Para superar el lógico miedo, que siempre provoca enfrentarse a una hoja en blanco, es importante considerar que existen al menos tres elementos esenciales que deben ser tenidos en cuenta para la definición de la política: la cultura de la organización, su marco normativo y el resultado del análisis de riesgos.

Respecto al primer aspecto, considero esencial el conocimiento de los principios y los objetivos que condicionan el funcionamiento de la organización, analizando para ello su misión, su visión y su mapa estratégico. Aunque la afirmación de que la "seguridad debe alinearse con los objetivos de negocio" es bien conocida y los conceptos que apoyan "el buen gobierno de la seguridad" cada vez están más implantados, no siempre se formulan de forma explícita.

Además, la legislación y la normativa que aplican a la organización deben ser contempladas en la política, aunque sea sutilmente, de forma que no se establezcan directrices que sean contrarias a ellas o que dificulten su cumplimiento.

Por último, deberíamos recoger el resultado del análisis de riesgos. En este punto, mi opinión es que hay que ser muy cuidadoso al determinar los objetivos a cubrir en este proceso y al delimitar su alcance. Es cierto que es un paso esencial, de "libro", pero no podemos caer en la trampa de realizar un análisis de riesgos demasiado ambicioso, que se prolongue en el tiempo y que nos lleve a "callejones sin salida". El análisis de riesgos es un medio y no un fin en sí mismo, y para el diseño de la política nos basta con una aproximación de "alto nivel".

Una vez identificado qué deberíamos conocer, estamos en disposición de "levar anclas" y ponernos a escribir. Al considerar los aspectos a incluir en la política no debemos perder la perspectiva de que, aunque generalista y de "alto nivel", lo que se recoja en ella condiciona profundamente el modelo de seguridad de la organización. Algunos aspectos que pueden ser incluidos, son:

- Directrices que deben ser tenidas en cuenta en cualquier actividad relacionada con la seguridad de la información, como: que el coste y el nivel de protección de un activo deba ser proporcional a la importancia que tiene para la organización, que formar y concienciar al personal en materia de seguridad sea una actividad estratégica o que la seguridad de la información deba ser evaluada periódicamente.
- Responsabilidades asociadas con la dirección de la seguridad de la información y los órganos necesarios para facilitar su desarrollo. En este apartado se podría incluir dónde se encuentra orgánicamente el departamento de seguridad, de quién depende y cómo se coordina con el resto de departamentos.

Estrategia

La estrategia que se debe seguir para que la política sea finalmente aprobada depende nuevamente de la complejidad de la organización pero, en todo caso, debería existir cierto nivel de consenso entre todos los departamentos. Para ello es imprescindible que el personal de seguridad involucrado en esta iniciativa cuente con ciertas habilidades: capacidad de negociación y de marketing interno; y que sean capaces de discernir entre lo prescindible y lo irrenunciable, de forma que puedan llevar "el buque a buen puerto".

Quisiera terminar este artículo siguiendo el estilo con el que lo comencé, por lo que me permitiré dar un par de "avisos a navegantes" (notificación de incidencias que ponen en peligro la navegación):

- Una buena política debe estar muy centrada en el negocio y en los requisitos específicos de cada organización y, por tanto, no sirven soluciones "estándar" que se reutilizan una y otra vez.
- Elaborar una política requiere conocimiento en gestión de seguridad de la información y grandes dosis de cultura organizacional, por tanto, es necesario conformar un equipo muy experimentado e involucrar activamente al personal de la organización.

Dicho lo cual, les deseo que tengan una buena singladura y vientos favorables. ■

Miguel Ángel Rego Fernández
Área de Seguridad
Inspección General CIS
MINISTERIO DE DEFENSA