# LAS RESPUESTAS A LAS SEIS PREGUNTAS (5W+H)

Para explicarnos algo siempre podemos recurrir de forma sencilla a las conocidas "Five Ws (and one H): Who, What, When, Where, Why, How". Cuando hablamos de la seguridad en una empresa se puede contestar a estas mismas preguntas, aunque en muchas ocasiones no sea tan sencillo y pueda variar de una empresa a otra. Solo si tenemos bien perfiladas las respuestas podremos gestionar esto de "la seguridad".

### What?

Hay que proteger sistemas, redes, infraestructuras, ordenadores, dispositivos móviles en todas sus variantes, información, servicios, edificios... toda una taxonomía. Además, el "What" tiene la costumbre de ser cambiante y puede ser tan amplio como se quiera, es cuestión de la profundidad a la que se considere llegar en el inventariado o identificación de activos. Si tenemos en cuenta la información en formato electrónico, esta tiene la propiedad de ser fácilmente copiada y la necesidad de ser compartida tanto dentro como fuera de la organización; es decir, el "What" se multiplica y está fuera de los límites de la empresa. Lo que preocupa es identificar y mantener un inventario de este "What", cuya complejidad y dispersión es directamente proporcional a la profundidad del mismo, así como a la complejidad organizativa y tamaño de la empresa.

### Why?

Una vez identificado el "What", se tiene que decidir por qué y cuánto se protege, atendiendo, por supuesto, a las necesidades del negocio. Para eso tenemos los análisis de riesgos, más o menos tediosos o *esquemáticos*, que nos justificarán por qué hay que implantar ciertas medidas de seguridad dependiendo del activo. En ocasiones, el seguimiento de un estándar o mejores prácticas nos evitará justificar lo que es obvio (para poner un antivirus no es necesario hacer un análisis de riesgos… ¿o sí?). Lo que preocupa es que el proceso de decisión o análisis de riesgos esté ajustado a las necesidades de la empresa y no llegue tarde a los "hechos consumados". Asimismo, preocupa relacionar los estándares y normas de seguridad que nos aplican: casi todos dicen lo mismo de diferente forma (es como la torre de Babel).

### How?

Para poner en práctica las medidas de seguridad identificadas anteriormente tenemos un variopinto mercado de tecnologías y fabricantes. Aquí tenemos que ser conscientes de que la tecnología no llega a todo y no nos quedará más remedio que procedimentar y organizar. También habrá que tener en cuenta la otra variante de la H, es decir, el "How much" de todas las medidas de seguridad que hemos identificado y justificado como necesarias. Lo que preocupa es acertar con la tecnología adecuada y entender sus limitaciones. También preocupa, especialmente en esta época de crisis, el coste de las mismas frente al resto de competidores. Si bien es verdad el dicho "lo barato termina resultando caro", también hay que considerar que "lo mejor es enemigo de lo bueno".

### When?

Y llegados a este punto tenemos que ver cuándo implantaremos las medidas de seguridad. En muchos casos será cuando los financieros de la empresa aprueben la partida presupuestaria, generalmente después de los recortes. En otras ocasiones, el limitante temporal lo establecerá la propia madurez de las tecnologías existentes. Lo que preocupa es cómo priorizar en el tiempo el siempre escaso presupuesto (¿qué dedo me corto que no me duela?).

> Muchos empleados justifican sus acciones apelando a la productividad y a la necesidad de hacer. Esto tenemos que entenderlo y hay que saber adaptarse a las necesidades actuales para que el área de seguridad no se convierta en el "doctor no", sino en el "doctor así no, sino de esta manera".

### Where?

Lo que queremos proteger puede estar abajo (bajo nuestro control) o arriba (en "las nubes"), aunque también puede estar en el medio. Ahora nos viene una avalancha de servicios para proyectos colaborativos en Internet, correo con cuota casi ilimitada en "la nube", redes sociales, etc. Otra vertiente es saber desde dónde aplicar las medidas de seguridad para proteger el activo. Aquí tenemos los servicios de seguridad gestionada en todas sus vertientes y modalidades. Lo que preocupa es cómo podemos medir y monitorizar la seguridad de los servicios externalizados, así como los procedimientos de actuación frente a un incidente de seguridad. No es suficiente confiar en las cláusulas de los contratos de externalización, pues las cláusulas en sí no protegen la información. Si existe un incidente de seguridad, nuestra empresa es la que realmente tiene el problema (aunque puedas involucrar o echar la culpa al proveedor por medio de las cláusulas).

### Who?

Lo hemos dejado para el final porque es lo que más puede o debe preocupar. Esta pregunta la podemos dividir en varias: ¿Quién es el responsable último de la seguridad de un activo de información? ¿Quién es el encargado de implantar las medidas de seguridad? ¿Quién las opera y administra? ¿Quién las monitoriza? En muchas normativas se dice que el responsable último de la seguridad de un activo es su propietario ("owner"), entendido como la persona o departamento que decide sobre la finalidad, contenido y uso del activo de la información.

Esta definición nos lleva a responsabilizar al empleado de la seguridad de la información que maneja. El problema común es que muchos empleados no se sienten responsables de la seguridad de la información empresarial que pasa por sus manos. La seguridad no es su problema y piensan que para eso están otras áreas, como el área de sistemas o de seguridad, máxime cuando ya existe una persona a la que han nombrado como "el responsable de seguridad", literal que puede llevar a engaño o a crear falsas expectativas en este sentido, pero que, sin embargo, viene "impuesto" por normativa.

En otros casos, muchos empleados justifican sus acciones apelando a la productividad y a la necesidad de hacer. Esto tenemos que entenderlo y hay que saber adaptarse a las necesidades actuales para que el área de seguridad no se convierta en el "doctor no", sino en el "doctor así no, sino de esta manera".

Cuando el empleado se siente responsable (que los hay) de la información que maneja, la empresa tiene que definir y difundir los procedimientos y poner a disposición las herramientas necesarias para que el empleado pueda ejercer esta responsabilidad de forma sencilla e intuitiva en función de la criticidad de la información. No podemos transferirle la responsabilidad sin darle los conocimientos y herramientas adecuadas. También se hace necesario definir las posibles sanciones internas en las que puede incurrir un empleado en caso de negligencia (quizás esto sea impulsado por la última reforma del Código Penal).

Por otra parte, está la división de funciones entre el área de seguridad de la información (entendida como fuera del área de tecnología) y el área de tecnología (donde puede existir la función del administrador de seguridad). Es fácil que cualquiera de las dos áreas esté tentada en hacer una integración hacia delante y realizar funciones que no le corresponden. Como norma general, es saludable una segregación de funciones entre la especificación de requisitos de seguridad, la operación y administración de las medidas de seguridad que los implementan, y la supervisión del cumplimiento. Lo que preocupa es que a los usuarios nos les preocupe esto de la seguridad o que exista una indefinición en las responsabilidades, tareas o funciones.

En resumen, para hacer algo lo más importante es saber quién lo tiene que hacer (y que quiera hacerlo). El qué, cómo, dónde, cuándo y por qué hay que perfilarlo junto con quién lo tiene que hacer. Hay un dicho popular que dice que se vive más despreocupado y feliz en la ignorancia, ¿implica esto que si queremos ser menos ignorantes tendremos que preocuparnos más? ■

**Juan Carlos Gómez Castillo**
Gerente de Seguridad de la Información
jcgomez@telefonica.es
**TELEFÓNICA ESPAÑA, S.A.**