MIKEL RUFIÁN ALBARRÁN. RESPONSABLE DE CIBERINTELIGENCIA; Y **PABLO BURGOS**. CONSULTOR DE CIBERINTELIGENCIA (I+D+I). INNOTEC SYSTEM

Ciberinteligencia: conocer para decidir correctamente

La incorporación de capacidades de Ciberinteligencia puede suponer un incremento de la rentabilidad de las organizaciones de hasta un 26%; sin embargo, en España, la apuesta por esta actividad es aún incipiente con respecto a otras grandes economías. Potenciar su desarrollo es imprescindible para maximizar las oportunidades que ofrece el nuevo entorno digital, valorar y mitigar los riesgos y lograr una posición ventajosa en el mercado.

Con la globalización, la digitalización y la conectividad, organizaciones de todo tipo de sectores se enfrentan al reto de identificar y aprovechar las oportunidades que ofrece el salto al mundo digital, así como las amenazas y los riesgos del ciberespacio.

En este sentido, las organizaciones están dedicando actualmente cada vez mayores recursos al examen de su entorno, con el fin de disponer de información útil y de calidad que les ayude en sus decisiones estratégicas, tácticas u operativas, con tres objetivos fundamentales: prevenir riesgos y amenazas, minimizar el impacto de las acciones de los competidores y lanzarse a la conquista de nuevas oportunidades en el ciberespacio.

Encontrar la forma de transformar sus estructuras, en muchos casos obsoletas, para hacerlas ciberinteligentes es el principal desafío al que se enfrentan las empresas e instituciones hoy en día.

Pero... ¿Qué es la Ciberinteligencia?

Es el producto obtenido tras aplicar a la información del ciberespacio distintas técnicas de análisis que permitan su transformación en conocimiento, de forma que resulte útil a la hora de tomar decisiones con el menor nivel de incertidumbre posible, siguiendo el ciclo de Ciberinteligencia **(Fig. 1)**:

1. **Dirección y planificación**: Establecimiento de los requisitos y planificación de las acciones.

2. **Recolección:** Recopilación de datos en bruto a través de las fuentes de información que hayan sido definidas en el proceso de planificación.

3. **Transformación**: Conversión de los datos en bruto obtenidos en formatos procesables y manejables que permitan su tratamiento y análisis.

4. **Análisis y producción**: Los datos tratados son procesados, enriquecidos, analizados y evaluados para extraer un producto de Ciberinteligencia, capaz de satisfacer las necesidades de la organización.

5. **Difusión**: Transmisión de la Ciberinteligencia producida en las fases anteriores y presentada en un formato fácilmente entendible a todos los niveles.

6. **Evaluación**: Valoración y retroalimentación de todo el proceso para su reevaluación y la mejora continua de todo el ciclo.

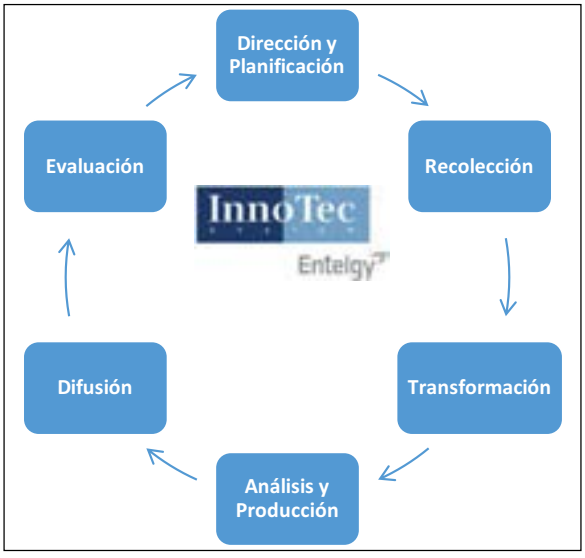

Fig.1. Rufián Albarrán, Mikel (2011). Guía profesional de Ciberinteligencia. Madrid

Con el fin de proporcionar un modelo preventivo y la mayor seguridad posible para una organización, los proveedores de servicios o células propias de Ciberinteligencia deben reunir los siguientes requisitos: **(Fig. 2)**

- Capacidad de explotación de las fuentes de información del ciberespacio.
- Cibercapacidades tecnológicas propias (Desarrollo I+D), que permitan reducir la dependencia externa de la organización en materia cibernética.
- Transformación de la información en inteligencia mediante un

Fig. 2. Rufián Albarrán, Mikel (2015). Manuel. Guía de Ciberinteligencia. Madrid Innotec System

equipo multidisciplinar con formación y habilidad en técnicas de análisis de inteligencia (Intelligence Analysis) y ciencia de datos (Data Science), para ejecutar análisis complejos de datos estructurados y no estructurados en plataformas y grandes volúmenes de información (Big Data) y de valor (Smart Data).

• Identificación de posibles violaciones a la identidad digital o propiedad intelectual, como puede ser el robo o falsificación de la documentación de uso interno.

• Conocimiento para evadir ataques a través de datos sospechosos y/o escondidos.

• Respuesta efectiva y rápida a situaciones de crisis.

• Comunicación en diferentes idiomas, ya que los ataques pueden provenir de cualquier parte del mundo.

• Servicio ininterrumpido 24x7, debido a que los atacantes suelen aprovechar los horarios de inactividad para realizar sus operaciones.

• Capacidad de ciberinvestigación (Detectives Digitales y Forense Digital) para la obtención y aportación de información con metodología forense.

• Elaboración de alertas tempranas e informes detallados para comunicar debidamente y con el objeto de reducir la incertidumbre en el proceso de toma de decisiones.

• Medidas de ciberdefensa para la protección de amenazas contra identidades digitales o contra infraestructuras de las organizaciones públicas o privadas.

El componente humano, factor clave

Aunque se empleen recursos informáticos para la producción de Ciberinteligencia, el análisis y la interpretación siguen siendo actividades esencialmente humanas. El analista de Ciberinteligencia es un especialista en la valoración, la integración, el análisis y la interpretación de la información en el ciberespacio para su conversión en conocimiento.

Carencia de cultura de Ciberinteligencia

Desafortunadamente, en España el desarrollo de estas unidades de Ciberinteligencia en la organización es reciente y nos encontramos aún lejos de los países precursores que son, además, las economías más competitivas.

Talento hay para ello, y es necesario apoyar y potenciar la Ciberinteligencia Nacional para salvaguardar la soberanía en el ciberespacio, compartiendo dicha Ciberinteligencia entre la comunidad, siempre y cuando sea oportuno.

La Ciberinteligencia no es un gasto, sino una inversión. Las organizaciones que la han incorporado son más competitivas, obtienen mayores beneficios y superan a sus homólogas en tres ámbitos clave: ingresos, rentabilidad y valoración del riesgo. Algunos estudios llegan a afirmar que las organizaciones ciberinteligentes son un 26% más rentables que sus competidoras. ●

Fotos: *Innotec System*

Contactos de empresas, p. 9.