# ¿Qué es la ciberinteligencia?

La ciberinteligencia es la recolección y análisis de información relacionada con amenazas y vulnerabilidades en el ciberespacio. Además de la recolección, también es la diseminación y la puesta en común de esta información para fortalecer a todos. La ciberinteligencia busca entender las potenciales ciberamenazas y los actores involucrados para permitir a las personas a cargo de la seguridad tomar decisiones informadas sobre cómo actuar y cómo prepararse ante un posible ataque.

## Etapas de la ciberinteligencia

La ciberinteligencia tiene 6 etapas:

1. Planificación: Se refiere a la coordinación de la operación de recolección de inteligencia. Definiremos qué información nos es útil, con qué herramientas, bajo qué criterios de calidad y de confiabilidad, y qué descartaremos o no nos interesa.
2. Recolección: Aquí se obtiene la información en bruto utilizando distintas fuentes y herramientas (de las que hablaremos abajo). Esta información está en bruto y todavía no está procesada.
3. Procesamiento: En este momento debemos normalizar la información. Es decir, convertirla en un formato legible, remover duplicados, desencriptarla, y ordenarla. La cantidad de información procesada requiere del uso de herramientas especializadas, como herramientas de análisis o visualización de datos, o una plataforma de inteligencia de amenazas (como ThreatConnect o SOAR).
4. Análisis: Con la información en formato legible, deberemos descartar aquello que no se adecue a los requerimientos que hemos definido en la etapa de planificación. En esta etapa es donde la información se convierte en inteligencia propiamente dicha y puede ser utilizada para los distintos fines de la organización. Existen dos tipos de análisis:
   1. Análisis táctico: Se centra en estudiar las tácticas, técnicas y procedimientos (TTP) de los atacantes, para poder desarrollar medidas o bloqueos contra ellos.
   2. Análisis estratégico: Se centra en estudiar las motivaciones de los ciberatacantes, y las tendencias generales del entorno ciber, para poder desarrollar medidas a largo plazo o evaluar dónde podrían atacar en el futuro.
5. Retroalimentación (o feedback): Esta es la fase donde utilizaremos la inteligencia propiamente dicha para tomar acciones y decisiones en nuestra organización. Es decir, trazar nuevos planes, generar nuevas defensas, ajustar prioridades, etc. También capacitaríamos a nuestro propio equipo de seguridad sobre nuestros descubrimientos.
6. Difusión: Una vez nos hemos beneficiado de esta información y ajustado nuestra propia organización, es momento de compartir esta información con el resto. Uno de los principios de la ciberinteligencia postula que somos más fuertes mediante la colaboración, y que evitarle a otro un ataque nos hace a todos más fuertes. Muchas veces, por ley, estamos obligados incluso a compartir esta información a una red centralizada como ser el CCN (Centro Criptológico Nacional) en España, por lo cual este paso es obligatorio.

## Fuentes de la Ciberinteligencia

La información recolectada para la ciberinteligencia viene de distintas fuentes:

* Datos abiertos o información pública, como aquella información publicada en portales de ciberseguridad o portales del gobierno de acceso público.
* Fuentes cerradas o información confidencial o clasificada, como documentos del gobierno de acceso privilegiado.
* Inteligencia técnica, que puede provenir de sistemas de monitoreo como un IDS o un firewall.
* Inteligencia humana: Información obtenida de las personas mismas, como las observaciones de los miembros del SO, o de los forenses cibernéticos luego de sus análisis.

Fuentes:

<https://snyk.io/learn/threat-intelligence/threat-intelligence-lifecycle/>

<https://masterenciberseguridadonline.es/que-es-la-ciberinteligencia-y-como-esta-estructurada/>

<https://telefonicatech.com/blog/las-fases-de-la-ciberinteligencia>