

Constructed examples of worst- case scenarios

**Ejemplos de hipótesis de riesgo más pesimistas**

## Examples of worst-case scenarios for various systems

There is a question in the questionnaire that asks the responder to define a reasonable worst-case scenario for a cyber attack on their system. The purpose of this question is to help the responder(s) be able to answer the impact related questions more accurately. The answer should be based on the likely threat actor, likely threat vector, and the most important of confidentiality, integrity, and availability.

These are four useful examples:

**Banking organisation: money service system**

* As a bank we care massively about the integrity and confidentiality of the money service system. It is a prized target for advanced cyber criminals, where new malware could defeat our defences. This could be used to extract millions of dollars, while pinning the blame on our customers.

**Telecommunications organisation: core network system**

* Our core telecommunications network is used by 100,000s of people every minute for business and personal needs, and they rely on it having high integrity and very high availability. We worry most about state actors using malware to reduce the availability of the network.

**Energy organisation: SCADA control system**

* Our SCADA system controls the electrical generating system for the whole country and must be highly available. We are most worried about our staff (Insiders) misconfiguring the system (accidents), as this could stop us matching supply with demand, or could damage the physical and expensive components of the electricity system.

**Government organisation: website system**

* Our tax collection website is the main portal for business tax collection and integrity and confidentiality are essential. We are most worried about cyber criminals and state actors trying to undermine the system using phishing attacks to allow malware in.

## Ejemplos de hipótesis de riesgo más pesimistas para diversos sistemas

Hay una pregunta en el cuestionario que pide al encuestado definir una hipótesis realista del peor caso posible de ciberataque a su sistema. El objetivo de esta pregunta es ayudar al encuestado a responder con más precisión las preguntas relativas al potencial impacto. La respuesta debe estar basada en el probable actor de la amenaza, el probable vector de la amenaza, y en los conceptos fundamentales de confidencialidad, integridad y disponibilidad.

A continuación, cuatro ejemplos útiles:

**Entidad bancaria: sistema de servicios monetarios**

* Como entidad bancaria asignamos suma importancia a la integridad y la confidencialidad del sistema de servicios monetarios, ya que es un blanco muy preciado para ciberdelincuentes expertos, y un ámbito en el que nuestras defensas podrían verse vulneradas por nuevos tipos de software malicioso. El ciberataque puede ser utilizado para extraer millones de dólares y culpar del hecho a nuestros clientes.

**Entidad de telecomunicaciones: sistema de red central**

* Nuestra red central de telecomunicaciones es utilizada por cientos de miles de personas a cada minuto para actividades laborales y necesidades personales, y los usuarios cuentan con que la red posea un alto grado de integridad y un muy alto grado de disponibilidad. Lo que más nos preocupa es que actores estatales utilicen software malicioso para reducir la disponibilidad de la red.

**Entidad energética: sistema de control SCADA**

* Nuestros sistemas SCADA controlan el sistema de generación de energía eléctrica de todo el país y por ende deben mantener un alto grado de disponibilidad. Lo que más nos preocupa es que miembros de nuestro propio personal desconfiguren el sistema accidentalmente, ya que esto podría impedirnos adaptar la oferta a la demanda o bien dañar los costosos componentes físicos del sistema eléctrico.

**Organismo gubernamental: sistema de sitio web**

* Nuestro sitio web de recaudación tributaria es el portal principal de recaudación de impuestos a la actividad económica. Su confidencialidad e integridad son esenciales. Lo que más nos preocupa es que ciberdelincuentes y actores estatales intenten socavar el sistema valiéndose de la suplantación de identidad para introducir software malicioso.