

Defining a suitable system for inclusion in the NCRA response

Definición de los sistemas sobre los cuales informar en el cuestionario de ENRC

## Defining a system for inclusion in the NCRA – Definición de qué sistema incluir en la respuesta al cuestionario de la ENRC

A successful NCRA relies on CNI organisations selecting the right system(s) to report on in their questionnaire response. This document aims to provide some help in making those system choices.

El éxito de la ENRC depende de que las organizaciones de infraestructura nacional crítica (CNI) elijan el sistema o los sistemas correctos sobre los cuales brindar información en el cuestionario. El presente documento tiene por objeto ayudar a elegir esos sistemas.

**Background information on systems - Información general sobre los sistemas**

A system is an organized, purposeful structure that consists of interrelated and interdependent elements. For example, components, entities, factors, members, parts etc.

Un sistema es una estructura organizada, concebida para un fin, que consta de elementos interrelacionados e interdependientes, p.ej. componentes, entidades, factores, miembros, partes, etc.

All systems:

* Have inputs, outputs, and feedback mechanisms.
* Maintain an internal steady state, despite a changing external environment.
* Display ‘emergent’ properties that are not possessed by any of the individual elements.
* Have boundaries that are usually defined by the system observer.

Todos los sistemas:

* Tienen productos de entrada y salida, y mecanismos de retroalimentación.
* Se mantienen internamente estables, aunque el ambiente externo sea cambiante.
* Muestran propiedades “emergentes” que no posee ninguno de los elementos individuales que lo componen.
* Tienen límites que habitualmente define el observador del sistema.

Systems stop functioning as intended when an element is removed or changed significantly.

Los sistemas dejan de funcionar de la forma pretendida cuando se elimina o cambia sustancialmente uno de sus elementos.

**Choosing Critical national Information Infrastructure systems – Elección de los sistemas de infraestructura de información nacional crítica**

When choosing a relevant system for the NCRA questionnaire consider:

* What business service this system is supporting
* How interconnected and vital it is to various other services or systems
* The scale on which it operates: from federated services to whole departments
* The purpose, features and behaviours that are being displayed
* How long it can be down before impacts start happening e.g. instantly, many weeks
* Whether the indirect consequences are interesting – e.g. social, business, welfare
* Whether this is a unique system or like many others.

A los fines de elegir un sistema apropiado para incluir en la respuesta al cuestionario de la ENRC hay que considerar:

* A qué área o servicio de la organización brinda soporte el sistema.
* Qué grado de interconexión o importancia tiene para otros servicios o sistemas.
* En qué escala opera (desde servicios federados hasta carteras ministeriales).
* La finalidad, las características y los comportamientos que exhibe.
* Cuánto tiempo puede estar sin funcionar hasta que se empieza a percibir el impacto (instantáneamente, varias semanas, etc).
* Si las consecuencias indirectas son de interés (sociales, operativas, de bienestar).
* Si se trata de un sistema único en su tipo o es igual a muchos otros.

**Some examples of potentially critical information infrastructure systems and reasons why – Ejemplos de sistemas de infraestructura de la información potencialmente críticos:**

* Energy: National grid mimic system: Shows all the energy flows and distribution resources in real time. Cyber interference could display erroneous data to maintainers who then make bad energy distribution decisions.

* Energy: Power plant control system: Controls all the different valves, turbines, generators, and transmission gear. Cyber interference could cause machinery to work outside of designed parameters, causing voltage and current drops, or failures in difficult to replace machinery.

* Finance: Real Time Settlement Systems: Ensure that monies traded between banks is always settled within a set period. Cyber interference could cause a bank to run out of money, a ‘run on a bank’, or negative credit rating changes.

* Finance: Cash dispensing system: Allows people to get access to physical money. A cyberattack could result in inability to access or provide criminals with all the money in multiple units.

* Telecoms: BGP routers. Ensure that data is correctly routed around the internet, enabling companies to do global business. Cyber-attack could enable man-in-the-middle attacks, sink-holing of data, redirection of traffic past espionage sniffing point.

* Telecoms: Core data network control system. Used to manage the servers and routers needed to manage the flow of data around an internet provider. Cyber interference could cause major network outages and the inability for data to be sent or received.
* Energía: sistema mimético de la red nacional. Muestra en tiempo real todos los flujos de energía y los recursos energéticos distribuidos. La ciberinterferencia podría hacer visualizar datos erróneos a los responsables del mantenimiento, quienes por consiguiente tomarían malas decisiones de distribución de la energía.
* Energía: sistema de control de usina eléctrica. Controla las distintas válvulas, turbinas, generadores y mecanismos de transmisión. La ciberinterferencia podría provocar que la maquinaria funcionara fuera de los parámetros establecidos, lo que a su vez ocasionaría una caída del voltaje y la corriente, o fallas en maquinaria de difícil reemplazo.
* Finanzas: sistema de liquidación en tiempo real. Asegura que las transacciones de dinero entre bancos siempre se liquiden dentro de un plazo establecido. La ciberinterferencia podría provocar que un banco se quedara sin dinero, o bien una corrida bancaria o una calificación crediticia negativa.
* Finanzas: sistema dispensador de dinero. Permite a las personas acceder a dinero físico. Un ciberataque podría impedir al usuario acceder al dinero o proporcionar todo el dinero de múltiples unidades a delincuentes.
* Telecomunicaciones: router BGP. Asegura el correcto ruteo de los datos en Internet, lo que permite a las empresas hacer negocios a escala mundial. Un ciberataque podría a su vez permitir ataques de intermediarios, desvío del flujo de datos, redireccionamiento del tráfico más allá del punto de interceptación de los *sniffers*.
* Telecomunicaciones: sistema de control de red central de datos. Se utiliza para manejar los servidores y routers necesarios para administrar el flujo de datos de un proveedor de Internet. La ciberinterferencia podría provocar una importante caída de la red y la imposibilidad de enviar o recibir datos.