

Handling and assessing NCRA responses

**Tratamiento y análisis de las respuestas al cuestionario de la ENRC**

## Summary of activities to do when receiving the NCRA responses

1. Collate data as soon as it becomes available, as this helps to see the patterns and gaps in the collected data.
2. Look for very similar / identical answers across responses from the same organisation that indicate a lack of thought e.g., vulnerability responses that are all the same.
3. Look for common systems in the same sector; there should be some. A missing system can be an indicator that not all systems have been identified, or an organisation isn’t willing to disclose.
4. Check that the systems are at a business service level e.g., systems to support services related to logistics, manufacture, sales, etc. The identified systems should not be something small like a networking component, unless this genuinely supports many services.
5. Compare NCRA responses with any security audit information you may have. There should be a correlation. If not, this could be a clue to ask for more information.
6. Put real energy and time into building the relationships with the organisations. The effort will be rewarded in terms of finding the right cyber security responses at a national level and continuing to have support from the organisations.

## Síntesis de actividades para realizar al recibir las respuestas al cuestionario

1. Compilar y ordenar los datos apenas estén disponibles, ya que esto ayuda a visualizar patrones de respuesta y datos faltantes.
2. Buscar respuestas muy similares o idénticas entre las proporcionadas por la misma organización que indiquen ausencia de reflexión sobre el tema, por ejemplo, igual respuesta a todas las preguntas sobre vulnerabilidad.
3. Buscar los sistemas comunes a un mismo sector. Debería haberlos. La falta de un sistema podría ser indicativo de que no todos los sistemas pertinentes han sido identificados, o que una organización no está dispuesta a divulgar información.
4. Verificar que los sistemas sean el soporte de las actividades principales de la organización. Por ejemplo, que los sistemas brinden soporte a servicios logísticos, de producción, de ventas, etc. Los sistemas identificados no deben ser algo pequeño como el componente individual de una red, a menos que dicho componente realmente sea el soporte de múltiples servicios.
5. Comparar las respuestas a la ENRC con cualquier información disponible de auditorías de seguridad. Deberían guardar relación. De lo contrario, esto podría servir de señal para solicitar más información.
6. Dedicar energía y tiempo a forjar relaciones con las organizaciones. El esfuerzo se verá premiado con la recepción de las respuestas adecuadas sobre ciberseguridad a nivel nacional y la continuidad del apoyo de dichas organizaciones.

## Checklist for assessing the quality of NCRA responses

* **Is the form complete?**

We would expect to see all the major questions answered, or ‘placeholders’ included for information that is to follow. The optional information may be provided but it is not essential.

* **Does it look as though what is completed look to be done accurately?**

We would expect there to be a good level accuracy e.g., the right words used, good spelling and punctuation for system names, and useful explanations and descriptions.

* **Has each organisation identified the range of systems expected?**

There are a variety of standard systems that could be viewed as critical, covering business, mission and safety; though some cover more than one area.

* **Is there a sensible range of answers per system?**

It is unlikely that all responses in each section will score the same e.g.

vulnerabilities, threats, etc. Therefore, check whether there is a spread of results.

* **Have conversations taken place with each organisation to help them complete the forms?**

Most organisations tend to benefit from a little help or clarification; or may already be seeking help to complete the questionnaires. In these discussions, additional confidence may have been gained from having:

* An appropriately senior person present
* Access to people with knowledge and experience
* Access to people in the right department who own the system
* A decent amount of time for discussion
* A sense of engagement and enthusiasm towards the NCRA
* People involved who have both ‘attention to detail’ and can see the ‘big picture’.

* **How do the similar system responses from one organisation compare to another?**

Given that some systems eg cash / accounting systems are found in many organisations, it can be useful to compare responses. This can help to get a sense for the level of risk appetite and basic levels of protection.

* **Based on experience, do any of the answers seem odd or unexpected?**

It is expected that the people reviewing the answers will have had some experience of the sectors, organisations and the systems within them. It should therefore be possible to make some ‘judgement calls’ on whether the answers seem sensible.

* **Are there any unusual or interesting systems reported?**

Many systems in an organisation could be classed as critical. It depends on the business, business model, organisational setup, risk posture, etc. However, if unusual systems are reported, it would be useful to check why they are included and possibly ask more about them. We usually expect just to see functional / service-based systems being classed as critical eg core network control system, accounting system, factory control system, generating control system, distribution system, software update system, etc.

* **Are any of the responses particularly high or low?**

If answers are too high, it could be a cry for help, wanting attention, or suspecting that funds will be made available to help the organisation; or that the organisation really has a genuinely high-risk system. While answers that all appear low could be indicative of an organisation in denial or wanting to cover up risks. Or perhaps the organisation really is managing its cyber risks.

* **Have the responses been validated by many people in their organisation?**

If the organisation can claim that their system owners, tech director or other responsible members have all helped to form the response, it is generally a good sign.

* **Has each organisation’s response been ‘signed-off’ at a senior level?**

Having a senior responsible owner for the response, who can authorise the release of the response, and claim that the right people have contributed to it, is a good sign.

* **Has the organisation reached out for clarification before submission?**

If the organisation had any doubts about the meaning of the questions, or what sensible responses should be, and has asked for clarification, then this is a good sign.

**Preguntas sugeridas para el control de calidad de las respuestas a la ENRC**

* **¿Está completo el cuestionario?**

Pretendemos que todas las preguntas principales sean respondidas o que se apunte que se proporcionará la información más tarde. Puede agregarse información opcional pero no es esencial hacerlo.

* **¿Las partes que se completaron parecen estar respondidas con precisión?**

Pretendemos un buen nivel de precisión, por ejemplo, uso de las palabras correctas, buena ortografía y puntuación en la denominación de los sistemas, y explicaciones y descripciones útiles.

* **¿Ha identificado cada organización la variedad de sistemas que se pretende abarcar?**

Hay una diversidad de sistemas que podrían considerarse críticos y abarcan actividades, misión y seguridad de la organización, aunque algunos abarcan más de una sola área.

* **¿Hay una variedad lógica de respuestas por cada sistema?**

Es improbable que todas las respuestas de cada sección (p.ej. vulnerabilidad, amenazas) arrojen un misma calificación. Por lo tanto, hay que verificar que exista una variedad de resultados.

* **¿Se mantuvieron conversaciones con cada organización para ayudarlas a completar el cuestionario?**

La mayoría de las organizaciones se benefician de recibir ayuda o aclaraciones, y algunas tal vez pidan ayuda desde un principio para responder al cuestionario. Estas conversaciones servirán para generar respuestas más confiables si:

* Está presente algún funcionario de alto nivel.
* Hay acceso a personas con conocimiento y experiencia.
* Hay acceso a personas del área correcta que sean las responsables del sistema.
* Se destina una buena cantidad de tiempo a la reunión.
* La ENRC genera compromiso y entusiasmo.
* Las personas involucradas prestan atención a los detalles pero al mismo tiempo tienen son capaces de adoptar una perspectiva general.

* **Si tomamos sistemas similares ¿qué respondió una organización en comparación con otra?**

Dado que algunos sistemas, p.ej. contables o de movimiento de efectivo, son comunes a muchas organizaciones, tal vez sea útil comparar respuestas. Puede ayudar a transmitir una idea del nivel de riesgo que una organización está dispuesta a aceptar y el nivel de protección básica que aplica.

* **En base a la experiencia ¿hay alguna respuesta que parezca extraña o sorpresiva?**

Se supone que las personas que revisan las respuestas tienen alguna experiencia de los sectores, las organizaciones y los sistemas que estas utilizan. Por ende, debería ser posible juzgar si las respuestas parecen razonables.

* **¿Se ha descripto algún sistema inusual o interesante?**

Muchos sistemas de una organización pueden ser clasificados como críticos. Dependerá de la actividad, del modelo de funcionamiento, de la estructura organizacional, de la postura frente al riesgo, etc. No obstante, si se describiera algún sistema inusual, sería útil verificar por qué ha sido incluido y tal vez pedir más información acerca de él. Generalmente son solo los sistemas funcionales/de servicios los clasificados como críticos, por ejemplo, sistema de control central, sistema contable, sistema de control de planta, sistema de control de generación, sistema de distribución, sistema de actualización de software, etc.

* **¿Alguna calificación del riesgo es muy alta o muy baja?**

Si una calificación del riesgo es muy alta, podría ser un pedido de ayuda o de atención, o una suposición de que servirá para que la organización reciba más fondos, o bien puede indicar la existencia real de un sistema de alto riesgo en la organización. Las calificaciones de riesgo muy bajas podrían ser indicativas de que la organización niega la realidad o pretende ocultar riesgos, o bien de que la organización realmente sabe manejar sus ciberriesgos.

* **¿Las respuestas han sido refrendadas por muchas personas de la organización?**

Si la organización puede afirmar que los responsables de los sistemas, el director técnico u otros funcionarios competentes han contribuido todos ellos a formular la respuesta, por lo general es una buena señal.

* **¿La respuesta de cada organización ha sido aprobada por algún funcionario de alto nivel?**

Que la respuesta sea responsabilidad de un alto funcionario que pueda autorizar la entrega del cuestionario y afirmar que han contribuido a responderlo las personas correctas es generalmente una buena señal.

* **¿La organización solicitó alguna información aclaratoria antes de entregar su cuestionario?**

Si la organización tuvo dudas acerca del significado de alguna pregunta o de lo que debería ser una respuesta lógica, y pidió información aclaratoria, esta es una buena señal.