

Getting the right core NCRA delivery team

Armar el equipo adecuado para la implementación de la ENRC

Delivering a National Cyber Risk Assessment (NCRA) requires a core team of people with the right range of skills, experience, qualifications, and connections. While there is not an exactly right answer, the information contained within this page should help you judge whether you are on track.

A team size of 5-10 people is normal. Any smaller and there will be too much to do. It takes energy and commitment to engage all the various Critical Information Infrastructure (CII) stakeholders. However, a larger team starts getting a bit too hard to manage and keep everyone focused, especially as they are sure to have other day-job requirements.

Cyber is a broad topic, with many areas where expertise is required e.g. cyber education, cyber defence, incident management, cyber systems development, vulnerability assessment, cyber audits, etc. Having people in your team who have worked in two or more cyber areas is a distinct advantage. Hopefully they have some cyber qualifications and certifications too e.g., ISO27000, SANS, Cloud competencies, Information & computer related degrees, etc. And even better if they know about existing national cyber policies, cyber frameworks, and ongoing cyber capability building activities.

The organisations that own CII are diverse and belong to many sectors e.g. telecoms, banking, energy, government, defence, transport, health, etc. It is advisable to have people in your team who are familiar with the cultures, processes, tools, and systems that are used in these sectors. We have found that people who have a role as a sector regulator or industry champion can be useful to have in the team. And they are likely to be friends with technical and managerial people in senior and middle management roles.

Much of the work in a NCRA is about ensuring that high quality and relevant data is obtained. You will want people in your team who can engage with those responsible for CII; who understand the intricacies of the CII systems; who like to help others understand the NCRA process; who want the best possible outcomes from the NCRA process; and who have the energy to see the job through.

Communicating is fundamental to achieving great results, building strong relations, and engaging constructively. There will be many briefings required during the workshops and in 1-2-1 sessions with the CII organisation representatives. It can sometimes take two or three attempts, using different words and pictures to explain what some of the cyber aspects mean and why relevant.

Data analysis is essential for the NCRA. The questionnaire responses are fed into one data analysis spreadsheet. You need at least one person in your team who can manipulate (Excel) spreadsheets. They will need to already know or learn the formulae, know how to manipulate the data, and be able to update and extract graphs and charts.

You need someone senior who can help you through any difficult periods e.g., when, for all your efforts, a few companies just won’t respond, or provide poor quality responses. Ideally, this will be your director or minister. And while not a day-to-day member of the team, they should have the gravitas and connections to reach and persuade CEOs and organisational leaders to engage more fully.

And finally, you will need a team leader who can manage all the aspects. Someone who can encourage and keep everyone together. Someone who sets high standards and ensures they are attained. Someone who is organised and can track the completion of the questionnaires. Someone who can assimilate information to create the report, and confidently present the NCRA findings to the CII organisation representatives.

Para llevar a cabo una Evaluación Nacional de Riesgo Cibernético (ENRC) se necesita un equipo central de personas dotadas de las habilidades, la experiencia, las calificaciones y las conexiones adecuadas. Si bien no existe una fórmula exacta, la información aquí provista lo ayudará a decidir si Ud. está bien encaminado.

Lo normal es armar un equipo de entre 5 y 10 personas. Si son menos, será demasiada la carga de trabajo. Se requiere energía y compromiso para trabajar con todos los actores de la infraestructura de información crítica. Al mismo tiempo, un equipo demasiado numeroso resulta algo complicado de manejar y dificulta la tarea de mantener a todos enfocados en la tarea, en particular porque seguramente tendrán otras exigencias que atender derivadas de su trabajo principal.

La cibernética es un campo extenso que abarca muchas áreas en las que se requieren conocimientos expertos, por ejemplo, cibereducación, ciberdefensa, manejo de incidentes, desarrollo de cibersistemas, evaluación de vulnerabilidades, ciberauditorías, etc. Tener en el equipo personas que hayan trabajado en dos o más áreas cibernéticas es claramente ventajoso. Sería deseable que también tuvieran alguna capacitación o diploma en la materia, por ejemplo, ISO27000, SANS, competencias digitales en la nube, un título en informática o computación, etc. y sería ideal que tuvieran conocimiento de las políticas y normativas cibernéticas nacionales y las actividades vigentes en materia de desarrollo de capacidades cibernéticas.

Las organizaciones que tienen a su cargo infraestructura de información crítica son diversas y pertenecen a múltiples sectores, por ejemplo, telecomunicaciones, bancos, energía, gobierno, defensa, transporte, salud, etc. Es aconsejable contar en el equipo con personas familiarizadas con las culturas, procedimientos, herramientas y sistemas que se utilizan en estos sectores. Hemos descubierto que aquellas personas que desempeñan funciones regulatorias o de promoción industrial en un sector son útiles para tener en el equipo, y probablemente ya estén vinculadas con personal técnico y directivo en cargos de gerencia media y alta.

Gran parte del trabajo de una ENRC tiene que ver con asegurar la obtención de datos de utilidad y de alta calidad. El equipo deberá estar integrado por personas capaces de vincularse con los responsables de la infraestructura de información crítica y entender las complejidades de los sistemas relacionados con dicha infraestructura; personas que deseen ayudar a otros a comprender el proceso que implica la ENRC, que pretendan obtener los mejores resultados posibles de la evaluación y que tengan la energía para ejecutar el trabajo de principio a fin.

La comunicación es fundamental para lograr buenos resultados, como también lo es construir relaciones sólidas y forjar un diálogo constructivo. Se requerirán muchas charlas preparatorias o instructivas durante los talleres y en las reuniones individuales con los representantes de las organizaciones vinculadas a la infraestructura de información crítica. A veces pueden ser necesarios dos o más intentos y utilizar distintas palabras e imágenes para explicar qué significan algunos de los aspectos de la evaluación y por qué son pertinentes a la tarea.

El análisis de datos es esencial para la ENRC. Las respuestas al cuestionario ingresan en una única planilla de cálculo para análisis de datos. Es necesario que al menos una persona del equipo sepa manejar planillas de Excel. Tendrá que conocer o aprender las fórmulas y el manejo de datos y ser capaz de actualizar y extraer gráficos y cuadros.

También se requerirá de un superior que ayude a transitar instancias difíciles, por ejemplo, cuando a pesar de todos los esfuerzos, algunas empresas simplemente no respondan o proporcionen respuestas de mala calidad. Lo ideal es que esta persona sea su director o jefe departamental y, si bien no formará parte del equipo diario de trabajo, tendrá el peso y las conexiones necesarias para llegar hasta los gerentes generales y presidentes de las empresas y persuadirlos de que participen más plenamente.

Por último, se requerirá un líder de equipo que pueda supervisar todos los aspectos, ofrecer motivación y mantener unido al grupo. Alguien que exija una alta calidad de trabajo y garantice que sea alcanzada. Alguien organizado y capaz de controlar que se completen los cuestionarios, alguien que pueda interiorizarse de la información para generar el correspondiente informe y presentar confiadamente los hallazgos de la ENRC a los representantes de las organizaciones vinculadas a la infraestructura de información crítica.