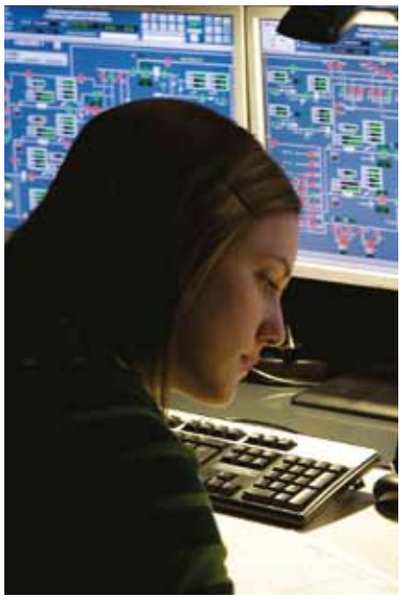
CIBERSEGURIDAD



Afrontando los riesgos digitales

En los años 90 los ataques informáticos eran meras anécdotas de personas que buscaban notoriedad. Conocidos como cibervándalos se dedicaban a crear virus molestos sin ningún beneficio. En la década pasada, el cibercrimen se abría paso a través de complejos programas con el fin de robar cuantiosas sumas de dinero. Recientemente hemos vivido el capítulo de un ataque dirigido sobre los sistemas de control de centrales nucleares en Irán. Hemos pasado del vandalismo informático de hace dos décadas al cibercrimen y todo hace pensar que en los próximos años debemos preparar nuestras infraestructuras contra el ciberterrorismo y la ciberguerra.

Los sistemas de control digital constituyen un componente crítico de la planta. A día de hoy, las necesidades de los usuarios invitan a aumentar la disponibilidad de los datos de proceso y por tanto a definir conexiones hacia la red de proceso. La tecnología utilizada está cambiando y el diseño de la planta evoluciona de sistemas propietarios, aislados y poco conocidos, a sistemas basados en tecnologías abiertas de uso común en TI y bien documentados en Internet, así como una mayor integración de los sistemas. Esta situación, aflora riesgos que hace algún tiempo eran impensables.

El número de incidentes ha crecido y los perfiles de los atacantes han pasado de ser meros individuos en búsqueda de notoriedad y satisfacción personal a grupos organizados que cuentan con grandes presupuestos e incluso intereses de los gobiernos de algunos países.

La ciberseguridad no es un aspecto meramente técnico, requiere involucrar a la organización y la definición de nuevas actividades y responsabilidades.

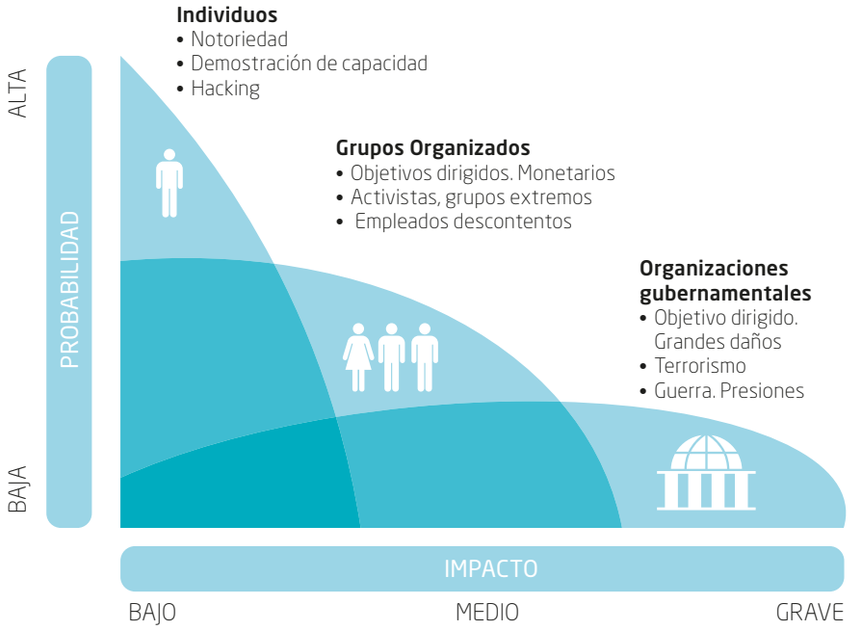
Para conseguir un nivel de ciberseguridad aceptable por una organización, es necesario conocimiento y experiencia en ambos mundos, el mundo del Control y el de la Seguridad de Sistemas de Información Tradicionales.

Los procesos de seguridad TI no son exportables directamente a los procesos de sistemas de control. Ni los requisitos de seguridad son los mismos ni la tecnología de seguridad es aplicable.

Indra, con capacidades y una extensa experiencia en ambos mundos (Sistemas de Control Industrial y Seguridad de Sistemas de Información) le ayudará a definir su plan de ciberseguridad teniendo en cuenta la definición de la estructura organizativa, identificando las amenazas y riesgos y proponiendo un programa de trabajo para asegurar la instalación desde el punto de vista de ciberseguridad.

Trece medidas para reducir el riesgo

1. Adoptar un marco de referencia.
2. Definir la organización, roles, actividades y responsabilidades de ciberseguridad.
3. Inventariar y clasificar los sistemas desde el punto de vista de ciberseguridad.
4. Análisis y gestión de riesgos.
5. Definir un procedimiento de gestión de incidentes de ciberseguridad.
6. Incluir los requisitos de ciberseguridad en cualquier proyecto desde el comienzo.
7. Concienciar y crear cultura.
8. Defensa en profundidad.
9. Implementar sistemas de defensa perimetral.
10. Planificar auditorías de ciberseguridad.
11. Monitorizar y correlar los eventos de los sistemas.
12. Gestionar adecuadamente las configuraciones de los sistemas.
13. Colaborar activamente en foros y grupos de trabajo especializados.



Anabel Segura 7
28108 Alcobendas
Madrid (España)
T +34 91 480 60 00
ciberseguridad@indra.es
www.indracompany.com