



PUNTO DE ENCUENTRO: CARTA DEL DIRECTOR

Protección de las Infraestructuras Críticas

Fiel a mi compromiso me vuelvo a dirigir a ustedes planteándoles un tema que me preocupa desde hace bastante tiempo «*La Protección de las Infraestructuras Críticas*».

Lo primero es definir qué entendemos por Infraestructuras Críticas. Son aquellas imprescindibles para el funcionamiento de los Sistemas de Información y Comunicaciones, de los que a su vez dependen de modo inexorable, tanto las Administraciones Públicas como las empresas, para cumplir sus funciones y alcanzar sus objetivos.

Todas las organizaciones responsables han tomado medidas para garantizar el adecuado funcionamiento de sus sistemas, estableciendo planes, realizando análisis de riesgos y aplicando los controles necesarios para garantizar dicho funcionamiento y, por ende, el de sus organizaciones. Estamos hablando de los Planes de Recuperación de Desastres, Planes de Contingencia y Planes de Continuidad de Negocio.

Pero las *Infraestructuras Críticas*, tienen una característica que las hace diferentes. Habitualmente no están bajo el control de la organización, que depende de ellas para su funcionamiento. No hay que olvidar que una *Infraestructura Crítica* da servicio a múltiples organizaciones. Estamos hablando de: energía eléctrica, telecomunicaciones, suministro de combustible, servicios de transporte, servicios sanitarios, seguridad...



by Guillermo Searle Hernández

RICARDO CAÑIZARES

Director de la Revista **a+**
director@revista-ays.com

Una
Infraestructura Crítica depende
a su vez de
otras
Infraestructuras Críticas y de
las TIC ...

Además hay que hacer notar, que a su vez una *Infraestructura Crítica* depende a su vez de otras *Infraestructuras Críticas* y de las TIC, que son imprescindibles para su gestión y entrega sus servicios. Estamos ante un círculo peligroso, un incidente en un sistema TIC de los que controlan una *Infraestructura Crítica*, puede provocar un cadena de incidentes en nuestra red de *Infraestructuras Críticas*, provocando una parada generalizada de sistemas TIC, que a su vez pueden provocar la paralización de las actividades productivas de multitud de organizaciones, que en el mundo global en el que nos encontramos puede afectar a todo un país, incluso a llegar a tener efectos en el resto del mundo.

No es mi objetivo plantear un caso concreto de incidente, que en caso de ocurrir pudiera poner en jaque a todo el tejido productivo de un estado, aunque en la historia reciente hemos tenido ejemplos de incidentes en *Infraestructuras Críticas*, que con interrupciones de servicio relativamente breves, han producido pérdidas cuantiosas, es fácil extrapolar lo que puede ocurrir en caso de la «caída» por un tiempo prolongado de una *Infraestructura Crítica*.

Los Sistemas de Información y Comunicaciones son imprescindibles para la existencia de nuestra forma de vida, hoy en día no sería factible el funcionamiento de nuestra sociedad occidental sin las TIC, todas las actividades de nuestra sociedad dependen de



las TIC, de una forma que hace unos años no éramos capaces de imaginar.

La sanidad, la banca, la Administración Pública, las comunicaciones, la distribución de alimentos, el transporte público y un largo etcétera, de actividades dependen de modo inexorable de las TIC, por no decir que no existe ninguna actividad que no dependa de alguna manera de las TIC. Si conocen alguna, les agradecería que me hiciesen el favor de comunicármelo.

En un mundo global e inestable en el que no ha tocado vivir, las amenazas a nuestra seguridad no entienden de fronteras, y nadie puede negar que las *Infraestructuras Críticas* de las que dependen nuestros Sistemas de Información y Comunicaciones, se encuentran expuestas a graves amenazas, que en caso de materializarse pueden provocar un colapso de nuestros Sistemas de Información y Comunicaciones.

Como el riesgo al que se encuentran expuestas las *Infraestructuras Críticas*, es función de la probabilidad de materialización de las amenazas existentes y del valor del impacto, la pregunta es ¿Cuál es la probabilidad de materialización de la amenaza?. No es fácil

responder a esta pregunta, pero el mundo global e inestable que vivimos, nos hace estimar un grado de probabilidad preocupante, y como el valor del impacto es muy alto, el riesgo del que estamos hablando es alto.

Si somos conscientes del riesgo al que están expuestas nuestras *Infraestructuras Críticas*, solo nos queda determinar que controles y salvaguardas hay que implantar para disminuir el riesgo a un nivel asumible. Pero estas tareas no son abordables aisladamente por una organización u organizaciones, es necesario una coordinación a nivel nacional para poder aplicar una adecuada política de protección de las *Infraestructuras Críticas*.

El Estado debe asumir la responsabilidad de garantizar la seguridad de las *Infraestructuras Críticas*, legislando, implantando políticas y procedimientos, y coordinando los esfuerzos de todas las organizaciones involucradas en el despliegue y gestión de las *Infraestructuras Críticas*.

Se deben adoptar las medidas necesarias para garantizar, bajo cualquier circunstancia, un nivel de funcionamiento de las *Infraestructuras Críticas*, que nos permitan mantener funcionando los servicios que se consideran esenciales para nuestra sociedad.

Me gustaría que reflexionaran sobre el impacto que sufrirían sus Sistemas de Información y Comunicaciones, en el caso de la materialización de una de las múltiples amenazas a las que están expuestas las *Infraestructuras Críticas*, y respondieran a la siguientes preguntas: ¿Su organización sería capaz de superar una eventualidad de este tipo? ¿Qué impacto supondría para las organizaciones con las que mantienen relaciones?

Nadie puede
negar que las
*Infraestructuras
Críticas* se
encuentran
expuestas a
graves
amenazas