ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

35/2015 03 de abril de 2015

*Luis de Salvador Carrasco**

CIBER-RESILIENCIA

Visitar la WEB Recibir BOLETÍN ELECTRÓNICO

CIBER-RESILIENCIA

Resumen:

Ciber-resiliencia es uno de los principios establecidos en la Estrategia de Ciberseguridad Nacional. La resiliencia es una cualidad inherente a un organismo, entidad, empresa o estado que le permite hacer frente a una crisis sin que su actividad se vea afectada. Dado la complejidad de las organizaciones y su dependencia de la infraestructura TIC, no se puede trazar una línea divisoria entre resiliencia y ciber-resiliencia. Alcanzar ambas implica realizar más que una gestión de la seguridad, hay que llevar a cabo modificaciones en la misma naturaleza de la organización, y desarrollar una infraestructura tecnológica segura por diseño. Se puede conseguir un determinado nivel de seguridad con políticas a corto plazo, pero para alcanzar una autentica resiliencia es necesario aplicar medidas estructurales a largo plazo.

Abstract:

Ciber-resilience is one of the principles stated in the National Cyber-Security Strategy. Resilience is an attribute of an organization, entity, company or nation that allows to face a crisis without a shutdown of organization processes. Due to the complexity of the current organizations, and their dependencies on the ICT infrastructure, it is hard to set boundaries between cyber-resilience and resilience itself. The way to reach both implies something more than the management of security. It implies to carry out changes in the organization constitution, and to develop a technical infrastructure secure by design. It is possible to reach an acceptable security level with short-term security policies, but it is necessary to develop long-term policies to get real resilience.

Palabras clave:

Resiliencia, Ciber-resiliencia, Riesgo, Ciberseguridad, Estrategia de Ciberseguridad Nacional, Cambio.

Keywords: Resilience, cyber-resilience, risk, cyber security, National Cyber Security Strategy, Change.

LA GESTIÓN DE LA SEGURIDAD

Todo organismo, empresa, organización o estado se ve sometido a tensiones derivadas de cambios e incidentes que se producen en su entorno, y también por eventos que se generan en su interior. Estas situaciones de estrés afectarán a los procesos de la organización en un grado que será tanto más grave cuanto más profundos, disruptivos o inesperados sean.

Una organización está formada por elementos humanos y materiales conectados entre sí mediante una red relaciones que puede alcanzar una gran complejidad. Un evento mínimo, interno o externo, puede desencadenar una reacción en cadena, produciendo un colapso de sus procesos, que evidenciará el desgaste que se ha producido en la organización a lo largo del tiempo debido a la operativa diaria. Muchas entidades sobreviven en estados de equilibrio muy precarios y una alteración, que se puede considerar pequeña en relación al tamaño del organismo o a la importancia de los procesos que ejecuta, puede precipitar una crisis.

Hace tiempo se llegó a la conclusión de que ninguna organización, por muy perfecta y sofisticada que sea, se encontraba libre de enfrentarse a situaciones que pudieran perjudicarla en mayor o menor grado, e incluso hacerla desparecer. Cualquier entidad se encuentra expuesta a una serie de amenazas, desde ataques hasta catástrofes, y es necesario implementar un conjunto de medidas que, con carácter preventivo, protejan a la organización frente a la materialización de dichas amenazas.

Las medidas preventivas proporcionarán una mayor seguridad y tendrán carácter organizativo, procedimental o técnico. De ahí se deriva que esas medidas de seguridad tendrán un coste, directo o indirecto, en la ejecución de los procedimientos de la organización. Lamentablemente, la relación entre el nivel de seguridad alcanzado y el número de medidas implementadas sigue el modelo de un diagrama de Pareto. El conjunto de medidas que se podrían adoptar, y por lo tanto el gasto, no tiene límite, se podría extender hasta el infinito sin conseguir la seguridad total. Esta carrera de incorporación de medidas es necesario detenerla en algún punto, un punto óptimo. La determinación de ese punto se consigue mediante un análisis de riesgos, que permite alcanzar el balance correcto entre el coste de las medidas y el hipotético beneficio obtenido por su implementación.

Este tipo de análisis utiliza una foto fija de la organización y del entorno el que se desenvuelve, pero ni uno ni otro son estáticos, sino dinámicos. Ambos evolucionan, de ahí que no solo es necesario implementar mecanismos que disminuyan el impacto o la probabilidad de un ataque o una crisis, es necesario implementar un procedimiento de adaptación constante de las medidas de seguridad mediante un análisis crítico permanente. Hay que ir más allá del análisis de riesgos y extenderlo a un proceso continuo que se conocerá como gestión del riesgo cuando se habla de amenazas, o gestión del cambio cuando se trata de la evolución ante la exposición a eventos externos.

Dentro de dicho proceso de gestión se tiene que asumir que, a pesar de todas las protecciones que se implementen, algunos de los ataques se materializarán con éxito y algunas catástrofes simplemente no se podrán evitar. Al ser la seguridad total un ideal inalcanzable, se ha de estar preparado para que el impacto, que inevitablemente se va a recibir, tenga una influencia mínima en la organización. Por lo tanto es necesario el despliegue, no solo de medidas preventivas, sino también de planes de contingencia que

cubran aspectos específicos para la continuidad de los procesos de la organización. Estas medidas correctivas, planes de continuidad de negocio, de recuperación de desastres y de gestión de crisis, también tienen el propósito de hacer disminuir el riesgo, y son de importancia vital en cualquier organización compleja.

RESILIENCIA Y CIBER-RESILIENCIA: QUÉ ES Y POR QUÉ

Una vez que se ha definido el marco para gestionar la seguridad de la organización, ¿qué aporta y en qué se diferencia el concepto de resiliencia? Los conceptos de resiliencia, seguridad y riesgo, o mejor, gestión del riesgo, son diferentes. En algunos casos sus fronteras se confunden porque, aunque sean distintos, no son independientes, sino que están relacionados. El concepto de resiliencia es más amplio que el de disminución o análisis del riesgo, pero este último forma parte de las estrategias para aumentar la resiliencia.

Resiliencia se define como una cualidad intrínseca, una característica propia de una organización que le permite enfrentarse de forma exitosa a los cambios y a los eventos tanto internos como externos. La resiliencia forma parte de la naturaleza de dicho organismo y está implícita en su estructura. Cuando una entidad se etiqueta como resiliente es porque se observa que ante una serie de sucesos la organización ha sabido reaccionar y externamente continua operando como si nada hubiera ocurrido. Por lo tanto, el término resiliente se puede aplicar tanto a una empresa como a un sector económico, a un gobierno, a un estado nacional o incluso un organismo vivo, a estructuras sociales como mercados, a comunidades o ejércitos.

Ciber-resiliencia se ha definido partiendo de la definición de resiliencia y restringiendo las posibles fuentes de crisis a eventos tecnológicos y procedentes del ciberespacio, o también se ha definido limitando la dimensión afectada de la empresa a lo que son sus sistemas de proceso de datos y sus comunicaciones. Dada la complejidad de las organizaciones, y la interdependencia entre los distintos elementos que las forman: personal, entorno social, suministros, infraestructura TIC, procesos, ...; no se puede trazar una línea divisoria clara entre lo que supone la resiliencia de la misma y la ciber-resiliencia de sus sistemas. Una y otra están íntimamente relacionadas, es más, son un mismo concepto. No se puede crear una infraestructura tecnológica ciber-resiliente si la organización en sí no es resiliente. La organización es un todo, y el departamento TIC no es un ente independiente que puede sobrevivir o pretender ser inmune a los eventos que pueden sacudir a su personal y sus usuarios.

El análisis de una organización desde el punto de vista del riesgo se basa en identificar vulnerabilidades una por una y fijar cada una de ellas. La gestión del riesgo tiene un límite. Llega un momento en que la naturaleza de la organización, de sus procedimientos, de sus procesos y la relación con su entorno no permite disminuir el riesgo ni ofrecer una garantía de continuidad por muchas medidas de seguridad que se implementen. Existe un punto a partir del cual, si se quiere alcanzar una mayor seguridad, lo que es necesario abordar es un cambio en los fundamentos de la propia organización. Cuando, añadiendo más elementos, más procedimientos, más técnicas, no se consigue disminuir los riesgos, sino al contrario, el sistema es cada vez más complejo y difícil de tratar, es cuando hay que estudiar cómo aumentar la resiliencia cambiando los principios rectores de la organización.

La rápida evolución de las amenazas implica que, utilizando soluciones específicas para cada una de ellas, siempre nos colocaremos en un plano de vulnerabilidad. Para evitarlo es necesario adoptar una aproximación basada en principios, como resiliencia. Esta es la medida de cuán poco vulnerable es una organización por su diseño, y la gestión de la resiliencia es la modificación de la naturaleza de la misma para llegar a lo que podríamos denominar "security-by-design", pero extendido desde el producto a la misma organización, pasando por cada uno de sus sistemas, consiguiendo una disminución de las vulnerabilidades por la propia concepción de la organización y de sus procesos. La resiliencia, y específicamente la ciber-resiliencia, se extiende a todos los dominios o planos desde los que se puede interpretar la organización: físicos, cognitivos, sociales, etc., y estos no se pueden tratar de forma individual, sino que se han de interpretar desde una visión unificada.

La gestión del cambio forma parte de la resiliencia de una organización. Una entidad será resiliente cuando se enfrente de forma exitosa tanto a los cambios que se desarrollan de forma progresiva, como a los que se desaten de forma violenta. Las alteraciones del entorno pueden ser desde ciberataques hasta catástrofes naturales, y podrían tomar cualquier otra forma: problemas energéticos, de suministros, políticos, financieros, contractuales, etc. Por otro lado, considerar que la única fuente de problemas puede ser un ataque externo es un gran error. El origen de una crisis que afecta de forma traumática a dicho organismo puede ser de origen interno. Centrar la estrategia en repeler ataques externos, subrayando la palabra ataques, es enfocar el problema de forma errónea. Una crisis interna puede generarse por la influencia de agentes externos o tener carácter mixto. Puede ser el caso de la crisis que se genera debido a una prolongada situación de estrés, condicionada por factores ambientales, que desgasta los recursos propios. En ese caso, los recursos más críticos son fundamentalmente humanos, sensibles a los fenómenos sociales. El personal en riesgo no es solo el equipo clave de toma de decisiones, puede ser parte del personal menos cualificado pero que son parte necesaria de los procesos de soporte de la organización. De especial sensibilidad son los mandos intermedios.

El concepto de resiliencia está íntimamente ligado con el concepto de sostenibilidad. En la mayor parte de los casos, los problemas internos que causan el colapso de una organización ante un escenario de crisis se encuentran latentes en la misma naturaleza y estructura de dicha organización. Por supuesto, antes del colapso se manifestarán problemas puntuales que se podrán señalar como síntomas, y dicho colapso comenzará por el punto más débil de la estructura. De ello se deduce que la capacidad de resiliencia no reside en una parte de la organización, no se puede señalar y acotar en un departamento o en una función. Aún menos es una capa o un barniz que se pueda extender en la superficie del organismo, ni es un escudo que se superpone a su estructura. La resiliencia forma parte de la propia naturaleza de la organización y está tan íntimamente ligada a ella que forma parte de su esencia.

Existirán grados en la capacidad de resiliencia de un organismo. Cuanto más traumática sea la crisis que es capaz de superar dicho organismo podemos hablar que es mayor su capacidad de resiliencia. Una crisis puede suponer una alteración transitoria de condiciones internas o externas, por ejemplo una huelga, un ataque informático o unas condiciones meteorológicas anormalmente adversas. Pero también puede suponer cambios permanentes, de carácter irreversible o con una duración prolongada en el tiempo. Puede

ser el caso de cambios políticos, de mercado, catástrofes naturales a escala regional o global. En el primer caso, la resiliencia se estimará en el grado en el que los procesos esenciales del organismo, los procesos de negocio en el caso de organizaciones, se vean afectados, y durante cuánto tiempo la organización puede seguir operando en esas condiciones, operando de forma efectiva, tal vez con una caída de rendimiento o de calidad que no sea de carácter esencial. En el segundo caso, en el caso de cambios permanentes, será más resiliente cuanto menos tiempo trascurra entre la crisis y la recuperación total del organismo, y cuantas más funciones estén operativas en ese lapso de tiempo.

Las organizaciones, todas en cuanto se consideran a largo plazo, se comportan como un organismo vivo. Ciertos cambios pueden originar un shock que paralice completamente su funcionamiento, o esta parálisis puede ser ocasionada por ciertas carencias. Cuando una organización se detiene tiene un plazo para reiniciar sus actividades antes de que el daño a la misma sea irreversible. La irreversibilidad supone pérdida permanente de capacidades o la desaparición de la misma. Este plazo de tiempo que mide el punto de no retorno es también una medida de resiliencia.

Resiliencia es un estado. El tener dicha cualidad implica que esa adaptación se ha de realizar en el mínimo intervalo de tiempo, a la máxima velocidad, incluso en tiempo real. Además, la recuperación debe implicar la continuidad de las funciones esenciales y la menor pérdida de capacidades. Por lo tanto, una organización resiliente es aquella con capacidad de toma rápida de decisiones, y también la capacidad del sistema para implementar dichas decisiones.

Resiliencia supone admitir que se producirán fallos, errores, y que tenemos los medios para restaurar la operación normal y asegurar los bienes y reputaciones. Por lo tanto, un aspecto importante que también mide el grado de resiliencia de una organización es su capacidad de anticipación a las crisis. Una justificación fácil es que las crisis o los ataques no son previsibles, que es imposible conocer cuándo se van a materializar, pero esto no es cierto. Excepto algunas catástrofes naturales y muy contados ataques, la mayor parte de las crisis de una organización se pueden prever, bien mediante un análisis de las series históricas, bien prestando atención a los sucesos en organizaciones similares, bien llevando a cabo una tarea efectiva de inteligencia o tan solo asumiendo lo que todos los días se lee en los periódicos.

Finalmente, una organización no será igual de resiliente a cualquier tipo de crisis. No es una cualidad que se pueda aplicar de forma homogénea en todas sus actividades o cada una de sus dimensiones. Un organismo puede ser muy resiliente a ataques técnicos, pero no a ataques sociales, o no muy preparada para crisis a corto plazo pero demasiado rígida para cambios del entorno a largo plazo.

RESILIENCIA COMO PRINCIPIO DE SEGURIDAD

La ciber-resiliencia aparece en primer lugar en la lista de las cinco prioridades y medidas del documento de Estrategia de Ciberseguridad de la Unión Europea[1], por delante de la

[1] Comunicación conjunta al Parlamento Europeo, al consejo, al comité económico y social europeo y al comité de las regiones. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro.

reducción del cibercrimen, el desarrollo de los recursos industriales y tecnológicos o del establecimiento de una política internacional coherente sobre el ciberespacio a nivel de la Unión Europea. El mismo documento desarrolla en el punto 2.1 los principios a desarrollar para alcanzar la ciber-resiliencia que se basan en la cooperación efectiva entre las entidades públicas y privadas, tanto a nivel nacional como a nivel europeo.

Esquemáticamente se pueden resumir como:

- Incrementar en la administración y las empresas los recursos dedicados a la prevención, detección y gestión de incidentes de seguridad. En este marco, el documento destaca el papel de ENISA para el desarrollo de técnicas para la seguridad y la resiliencia de sistemas industriales, de suministro y transporte. Otro aspecto importante es la implementación de medidas de protección de los datos de carácter personal y, en particular, aborda la necesidad de que los operadores de telecomunicaciones desarrollen procedimientos de gestión del riesgo y de notificación de brechas de seguridad.
- Armonizar la legislación y las instituciones de los distintos países europeos. Esto implica el desarrollo e implementación de una política de seguridad en redes e información (NIS), así como la creación de una Autoridad Nacional, la activación y coordinación de CERTS, en particular los de las instituciones europeas, y con herramientas de prevención y reacción también coordinadas.
- Incluir en este esfuerzo las empresas privadas, como entidades que tienen en sus manos gran parte de los recursos informáticos, con herramientas legales que obliguen a las organizaciones de sectores estratégicos (financieros, suministros, etc.) a alinearse con las estrategias definidas para el sector público. Entre estos, la notificación de brechas de seguridad que afecten a los procesos básicos de prestación de servicios.
- Impulsar la cooperación de las Autoridades NIS con, por un lado, las Autoridades de Protección de Datos y con las Fuerzas y Cuerpos de Seguridad, y, por otro lado, con el sector privado sobre la base de iniciativas que vayan más allá de las obligaciones legales, como es el European Public Private Partnership for Resilience (EP3R)[2].
- Realizar ejercicios a nivel europeo para comprobar el nivel de ciber-resiliencia y la efectividad de las medidas anteriores.

Como no podría ser de otra forma, la Estrategia de Ciberseguridad Nacional también trata sobre la ciber-resiliencia. En concreto, aparece en los dos primeros de los seis objetivos específicos que se fijan en el texto[3] y que se reproducen a continuación:

> *"1) para las Administraciones Públicas, garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por estas poseen el adecuado nivel de seguridad y resiliencia;*

Alta representante de la Unión Europea para Asuntos Exteriores y política de seguridad. Comisión europea Bruselas, 7.2.2013 JOIN(2013) 1 final.

[2] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

[3] Estrategia de Ciberseguridad Nacional 2013 Presidencia del Gobierno

2) para las empresas y las infraestructuras críticas*, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular; "*

Las acciones que se plantean para alcanzar la ciber-resiliencia comienzan por la disponibilidad de productos confiables, a través de la potenciación, el impulso y el reforzamiento de las capacidades nacionales de investigación y desarrollo en ciberseguridad de las TIC. Los objetivos anteriores se desarrollan a lo largo del texto y aparecen en las distintas líneas de acción esquemáticamente como sigue:

- Actualización del marco jurídico con el desarrollo de un marco nacional, coherente e integrado de políticas, procedimientos, estándares y normas de seguridad de aplicación tanto en el sector público como privado.
- Implantar en las AA.PP. de servicios de seguridad para la prevención, detección y respuesta a incidentes, en un proceso de mejora continua.
- Impulsar la cooperación y el intercambio de información entre la industria y los servicios de ciberseguridad.
- Desarrollo y mejora de herramientas, en particular de los sistemas militares, de inteligencia y aquellos que soportan los sistemas de comunicaciones de importancia estratégica. Estos últimos en cooperación con los operadores privados.
- La protección del Patrimonio Tecnológico.
- Potenciar la red SARA
- Asegurar la implantación de la normativa sobre infraestructuras críticas.
- Potenciar el CERT de Seguridad e Industria, en particular su cooperación con el CNPIC, las FyCSE y otros órganos de respuesta a incidentes.
- Desarrollar modelos de simulación para el estudio de las dependencias y riesgos de la infraestructuras críticas

Fuera del entorno europeo, podemos destacar la Orden Ejecutiva 13636 del presidente Obama y la Directiva de Política Presidencial 21, que destaca la necesidad de aplicar los principios de resiliencia en las infraestructuras críticas como defensa ante los ciberataques. Las líneas estratégicas que señalan son:

- Clarificar y refinar las relaciones funcionales entra las distintas agencias federales para avanzar en la unidad de esfuerzos que permitan fortalecer la seguridad y la resiliencia de las infraestructuras críticas.
- Permitir un intercambio eficiente de información, incluyendo inteligencia, mediante la identificación de la información y requisitos básicos necesarios para el Gobierno Federal.
- Implementar funciones de análisis que permitan tomar decisiones operativas y de planificación en relación a las infraestructuras críticas.

A estas líneas añade la necesidad de potenciar la investigación y desarrollo en las tecnologías de las infraestructuras críticas, en particular las relativas a seguridad. Dicha orden termina estableciendo medidas concretas y plazos para su ejecución, que han servido

como punto de arranque de diversas iniciativas específicas en ese sentido desarrolladas por el Gobierno Federal[4].

CÓMO ALCANZAR LA CIBERRESILIENCIA

En el apartado anterior se han mostrado las estrategias que, para alcanzar la ciber-resiliencia, se plantean en las iniciativas europeas y españolas sobre ciberseguridad. A continuación se desarrollan algunos de sus principios.

La resiliencia forma parte de la esencia de la propia organización. Pretender que la infraestructura TIC sea ciber-resiliente sin tocar la parte más íntima de toda la organización es una utopía. Esto supone ir más allá de la de los sistemas, redes, bases de datos, aplicaciones… procedimientos, todos ellos, directamente relacionados con los servicios de informática. Para conseguir la ciber-resiliencia hay que modificar la misma naturaleza de los procesos, del personal y de la infraestructura de toda la organización[5].

El primer paso antes de tomar alguna medida para incrementar la ciber-resiliencia es alcanzar un conocimiento real y profundo de la organización y su entorno. Aunque parece una afirmación muy evidente, es poco frecuente que se conozca la realidad de la organización, y menos a nivel directivo. Los manuales de operación de las empresas ofrecen una imagen idealizada del funcionamiento de las mismas, que siempre se encuentra muy alejada del modo real de trabajo, y no reflejan la multitud de canales ocultos y relaciones que constituyen las operaciones de su día a día. Para conseguir una visión crítica de la organización no solo es necesario obtener la visión desde dentro, es de capital importancia obtener información de cómo la misma se aprecia desde el exterior. Esa visión la proporcionan aquellos que tienen que interaccionar con ella, ya sean clientes de sus servicios o competidores.

La adecuada gestión del riesgo, la gestión del cambio y la implementación de medidas preventivas y correctivas en toda su extensión, incluyendo planes de continuidad de negocio y de recuperación frente a desastres, forman una parte capital de las herramientas para aumentar la ciber-resiliencia. De entre ellas, hay que destacar la palabra "cambio", que es una de las que más aparecen a lo largo de este texto. Una organización resiliente es la que incorpora el concepto de cambio como parte de sus principios de su funcionamiento.

Como en cualquier estrategia de ciberseguridad, la resiliencia descansa en gran parte en el factor humano. En este caso, principalmente en la capacidad ejecutiva, el liderazgo y la concienciación. Una dirección con conocimiento, una conciencia de la organización, sus procesos, sus fortalezas y sus limitaciones es vital, es decir, una dirección integrada en la organización. Esto supone una dirección realmente informada, o con capacidad y voluntad de informarse, de cada uno de los procesos que se ejecutan en la organización y que pueda tener una visión global desde lo pequeño a lo grande. Una figura clave será el responsable de ciber-resiliencia con voz a nivel directivo[6]. Toda organización es un ente dinámico que

[4] Como por ejemplo el *Improving cybersecurity and resilience through acquisition del DoD* http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf

[5] Bahadur, A. V., Ibrahim, M., & Tanner, T. (2010) *The resilience renaissance? Unpacking of resilience for tackling climate change and disasters*. Institute of Development Studies (for the Strengthening Climate Resilience (SCR) consortium): Brighton, UK

[6] Ya se encuentran en Linked-in puestos de trabajo específicos para la gestión de la ciber-resiliencia

modifica y crea nuevos procesos, productos o servicios. Cada uno alterará la red de dependencias de la organización y tendrán que ser estudiados por la dirección sobre cómo afectan a la resiliencia del todo.

Como principio de seguridad que es, la concienciación del personal de la organización es un aspecto de capital importancia. Pero para alcanzar un nivel adecuado de resiliencia se necesita algo más que concienciación, se necesita el compromiso real del personal[7]. Si, por un lado, en los últimos años se ha puesto de moda la necesidad de fidelización de los clientes, por otro se ha abandonado la fidelización del personal. Al abandonar el compromiso de la organización con los trabajadores, estos abandonan el compromiso con la organización y se convierte en una relación de carácter utilitarista a corto plazo y en ambos sentidos. Los resultados son aún peores cuando la falta de fidelización se produce a nivel directivo. Para crear este compromiso mutuo la organización ha de ofrecer una carrera profesional a sus trabajadores, más aún, un plan de vida, una seguridad, un sentimiento de grupo, en algunos casos un ideal, y una proporcionar una serie de valores añadidos que vayan más allá del estímulo económico directo.

Por otro lado, esa comunidad de intereses entre el personal de la organización y la organización misma no se podrá lograr si no existe al menos un cierto grado de cohesión social de los individuos fuera del entorno de la organización. Difícilmente se conseguirá este objetivo si en el equipo de trabajo existe personal con problemas de segregación, exclusión, auto-exclusión, polarización ideológica o fanatismo. Indudablemente, una organización será un reflejo de la estructura social en la que se inserta.

La capacidad de anticiparse a las crisis es un aspecto clave en la resiliencia de cualquier organización, de ahí la importancia de los CERT y la necesidad de potenciarlos en su capacidad proactiva y anticipatoria de amenazas, no solo en su carácter reactivo. Esa capacidad no se puede obtener si no es observando críticamente el estado del entorno y su evolución. Para ello, la organización ha de llevar a cabo una auténtica labor de inteligencia. Será necesario un grado elevado de permeabilidad en las voces que participen en el proceso de toma de decisiones que permita un flujo real de información de abajo hacia arriba, hacia los niveles de toma de decisión. También un alto nivel de conectividad entre unidades que permita el intercambio de información, conocimiento y aprendizaje. Una intercomunicación que no suponga dependencia, sino que esté ordenada de forma que permita anticipar y gestionar el proceso del cambio. La capacidad de anticipación no es solo una cuestión de información, sino de actitud. La dirección de la organización ha de ser consciente de que no controla todas las variables y ha de estar preparada para esperar lo inesperado, y con la flexibilidad mental de aceptarlo antes de que sus consecuencias sean irreversibles. La capacidad de pensar «out-of-the-box», permitirá ser proactivo y explorar nuevas y novedosas opciones para enfrentarse a lo incierto y lo inesperado.

Una organización resiliente será aquella en la que el árbol de relaciones humanas y materiales que la conforman sea lo más sencillo posible. Un aspecto clave para lograr la

[7] Coyle T., "Your Best Asset? An Empowered and Aware Workforce", CIO, enero 2014 http://www.cio.com/article/2865519/security0/your-best-asset-an-empowered-and-aware-workforce.html?utm_campaign=sflow_tweet#tk.rss_all

ciber-resiliencia es la simplificación de la organización, y en particular de sus sistemas de información. Una organización más simple es aquella que lleva a cabo menos procesos, en menos unidades, con menor diversidad de sistemas y con menos interfaces entre ellos y, sobre todo, con el exterior. Si la estructura de la organización es muy compleja, y la dependencia entre sus sistemas es alta, será muy difícil determinar el grado de impacto que un evento simple puede tener en la operativa global de la misma, ya que será imposible obtener un modelo realista de su funcionamiento. En entidades complejas el efecto de un evento tendrá un comportamiento que se alejará de ajustarse a un modelo lineal y se acercará más a un modelo caótico. Es muy difícil tratar con dichos modelos, menos aún de forma analítica, y predecir su comportamiento. Pero lo que sí es posible es simplificar una organización dividiéndola en unidades con interfaces bien definidos, en las que se pueda estudiar su comportamiento mediante modelos más simples. Cada unidad por separado tendrá ante un cambio un comportamiento más cercano a un modelo lineal y aumentado la latencia de sus interfaces, es decir, la velocidad con la que una crisis se propaga entre sus unidades, se conseguirá una organización más fácilmente controlable y predecible.

Una organización resiliente será aquella en la que sus procesos continúen operativos en cualquier circunstancia, con un grado de eficacia que tal vez no alcance el cien por cien del rendimiento deseable, pero que sí permita mantener la vida de la organización. Ante una incidencia es necesario distinguir aquellos procesos que son imprescindibles, frente a los que se pueden detener temporalmente, clasificando estos últimos en función del tiempo que pueden estar suspendidos (algunos podrán estar detenidos durante minutos otros indefinidamente) desarrollando un plan de continuidad de negocio a largo plazo y con una visión amplia. Para ello es necesario identificar cuáles son los recursos claves, y en particular los recursos TIC, que son imprescindibles para mantener el funcionamiento de cada uno de ellos. En función de dicha clasificación, realizar una matriz para determinar una asignación de recursos a procesos utilizando criterios de criticidad dentro del plan de recuperación de desastres. Así mismo, los recursos, en particular los recursos humanos, han de ser lo suficientemente flexibles para ser asignados dinámicamente de un área a otra, lo que exige preparación, ensayo y dirección.

Dentro de este plan hay que tener especialmente en cuenta los interfaces externos, que están formados por toda relación que tiene la organización con su entorno. Los interfaces con el exterior son de muchos tipos, pueden abarcar desde aspectos sociales a las redes de suministro eléctrico, pasando por el outsourcing y los servicios en la nube. Una estrategia de ciber-resiliencia ha de estar dirigida a disminuir las dependencias externas. Esto no quiere decir que una organización sea autárquica en su operativa diaria, es imposible imaginar una organización completamente aislada, y el aislamiento no tiene que ser el objetivo de una organización, ya que perdería su sentido. Pero ha de ser capaz de resistir durante un periodo de tiempo tan prolongado como sea posible cortes en los suministros, en especial en los suministros de energía, y no ha de depender en su operativa de servicios proporcionados a la propia empresa a través de Internet. En particular, todos los procesos de negocio han de poder llevarse adelante utilizando los servicios propios de la organización: telefonía, correo, compartición de documentos, sistemas de gestión, base de datos, etc. Más importante, la organización debe disponer del capital humano y del know-how necesario para realizar dichas tareas. Es más fácil reponer máquinas que reponer profesionales, tanto para la

operación, como el mantenimiento y el desarrollo. Ellos son la parte capital del Patrimonio Tecnológico de una organización o de un país.

Un aspecto a destacar es que cada vez tienen más peso la naturaleza social de los trabajadores de la organización. En un mundo global, las dependencias sociales y los miembros de la organización no se centran en un entorno geográfico inmediato, sino que tienen un alcance global mediante las redes sociales, redes de contactos, mensajería instantánea, etc. De esa forma, los sucesos que ocurren en todo el mundo entran directamente en la organización a gran velocidad. Una catástrofe en Malasia o un atentado en Nueva York afecta al rendimiento y las decisiones de los miembros de la organización. La información y los sentimientos sociales entran a través de los dispositivos personales, por lo que el BYOD[8] no es solo una amenaza técnica, sino una amenaza social. Esto no supone despreciar virus y troyanos que puedan penetrar utilizando mensajes o conectando elementos de control, como no hay que minimizar la información que se filtra al exterior utilizando los mismos elementos mediante metadatos o elementos más evidentes, como son fotografías realizadas en las propias instalaciones o conversaciones sobre aspectos internos e inmediatos sobre la organización y su personal.

La reducción de dependencias externas ha de estar ligada también a la reducción de dependencias internas. Esto implica que la organización ha de implementar redundancia en sus sistemas, en su personal y en sus procesos. Por principio, se ha de evitar exponer cada uno de los elementos claves de la organización a las mismas amenazas, y, por otro lado, los elementos que incorporan redundancia distribuirlos por los mismos criterios: localización geográfica, de tipo de aplicación, de fabricantes, de suministradores de red de comunicaciones, de personal e incluso de órgano director. En conclusión, balancear el riesgo entre todos los elementos de la organización.

Los procesos de la empresa se construyen sobre el sistema de información de la organización, cuyos ladrillos los forman un conjunto de hardware y software suministrado por diferentes proveedores. Si el objetivo es conseguir el «security-by-design» de la organización y de su infraestructura TIC, será necesario garantizar el «security-by-design» de los elementos que soportan los procesos de la empresa. Actualmente, los requisitos establecidos para la adquisición de sistemas y de aplicaciones van poco más allá de las descripciones funcionales. De hecho, se aceptan unas desviaciones muy grandes en la funcionalidad y la fiabilidad de los sistemas TIC y se hace descansar la seguridad del conjunto en las estrategias de detección y reacción ante sus brechas. Para conseguir una auténtica resiliencia no debe existir una línea que divida la parte funcional de la parte de seguridad en cada producto, y para ello es necesario aumentar el nivel de exigencia en la compra de los elementos de nuestra infraestructura. El objetivo último es conseguir una verificación formal de las especificaciones de los productos, especificaciones orientadas a la seguridad en un entorno ciber-hostil, que permitan demostrar «a priori» la seguridad de los diseños. Este no es un camino fácil, supone cambiar la cultura en el entorno de ingeniería de desarrollo, así como en la ingeniería de requisitos ligada a la adquisición de productos.

[8] BYOD: Bring Your Own Device. Denominación que se ha dado a la utilización del dispositivo de comunicación personal del trabajador con fines laborales.

Relacionado con lo anteriormente expuesto está la necesidad, como en la estrategia de ciberseguridad se planteaba, de proteger y potenciar el patrimonio tecnológico. No solo proteger el capital humano, que ya se ha comentado, sino también el patrimonio material. Esto supone algo más que tener un depósito de material de reserva de dispositivos que son para nosotros cajas negras. Para conseguirlo de una forma realmente sostenible es necesario impulsar las tecnologías propias y mantener una industria nacional que reduzca todas las incertidumbres relacionadas con las cadenas de suministro o con especificaciones ocultas. Y esto hay que hacerlo más allá de los productos específicos para implementar sistemas de seguridad, lo que supondría centrarse únicamente en el aspecto reactivo, sino en toda clase de sistemas para que la infraestructura tecnológica sea segura por diseño.

LA GESTIÓN DE LA CIBER-RESILIENCIA

Intuitivamente es fácil adivinar que medir la resiliencia de una organización no es algo inmediato, pero un concepto que no se puede medir, analizar o contrastar carece de utilidad práctica, ya que en ese caso no se podría gestionar de forma racional. Es necesario desarrollar un modelo analizable de forma objetiva, preferentemente cuantitativa, que tenga una aplicación práctica real, que permita realizar comparaciones, y del que se puedan extraer reglas e inferir resultados. En otro caso el concepto de resiliencia caería víctima de las interpretaciones no rigurosas y modas.

No es posible medir de forma directa un concepto que entraña gran complejidad. La resiliencia es una variable compleja imposible de derivar de una lectura sencilla y directa de una organización. El hecho de que la ciber-resiliencia implique la capacidad de adaptación y supervivencia a cualquier tipo de cambio supone que se ha de estudiar la organización, y su relación con el entorno, en todas sus dimensiones. Esto supone recoger una serie de indicadores y medidas cuantitativas, de muy distinto tipo, que serán sistematizadas en una serie de métricas que permitirán tener una caracterización de la organización como un todo y de cada una de sus partes. Han de emplearse métricas de ingeniería, de toma de decisiones, sobre distintas tecnologías y niveles de abstracción, de seguridad y de otras disciplinas, así como métricas desarrolladas ad-hoc. En el caso de ciber-resiliencia, es necesario que dichas medidas reflejen no solo el estado de los procesos dependientes de la infraestructura TIC de forma estática, sino las relaciones dinámicas entre los elementos de la organización y el entorno: el conjunto de elementos físicos que lo conforman, los flujos de información, el plano cognitivo y el de relaciones sociales inter y extra organización[9]. Estas medidas han de incluir métricas de coste que permitan evaluar el gravamen que supone implementar una determinada estrategia de ciber-resiliencia, una solución concreta, un producto o sistema o un cambio en los procesos de la organización. La medida del coste también será multidimensional, ya que tendrá en cuenta no solo el coste directo de la integración de la solución, sino también los costes de mantenimiento y su impacto en el conjunto de procesos y estrategias de la organización. La ciber-resiliencia no se evaluará como un todo o nada. Una organización tendrá un grado determinado de resiliencia que se

[9] Igor Linkov, Daniel A. Eisenberg, Kenton Plourde, Thomas P. Seager, Julia Allen, Alex Kott. Resilience metrics for cyber systems. Environment Systems and Decisions, 2013; DOI: 10.1007/s10669-013-9485-y

determinará en función de cómo se vean afectados los procesos de negocio, o aquellos esenciales para la operación de la empresa, y por cuánto tiempo.

Una vez obtenida una medida, será posible determinar qué mejoras se pueden introducir en la organización para incrementar el valor medido de resiliencia. Con las mejoras implementadas, incluyendo los cambios que de forma paralela se han producido en el proceso de adaptación, se podrá tener una estimación de si la organización ha mejorado su capacidad de resiliencia y compararla con otras organizaciones similares de su entorno. Para cada uno de los elementos a medir es necesario definir cuáles son los niveles de servicio deseables y, a partir de ellos, determinar cuáles son los niveles aceptables, medidos a su vez de forma cuantitativa, de forma directa a través de determinados parámetros de calidad o indirecta a través de la medida del impacto que tiene la interrupción del servicio. La estimación de los niveles aceptables de servicio es capital, no solo para la medida de la resiliencia. Implementar una organización resiliente tiene un coste a corto plazo, y es necesario medir con precisión la carga que supone alcanzar dichos niveles, de igual forma que en un análisis de riesgos.

En este artículo no se pretende fijar un modelo de medida de resiliencia, pero sí dar algunas indicaciones bibliográficas sobre los trabajos que se han desarrollado para obtener un marco de referencia para la elaboración de un conjunto de métricas de resiliencia[10]. Entre ellos cabe destacar los estudios realizados por ENISA en su programa para la evaluación de la resiliencia en infraestructuras críticas[11] [12], el desarrollo de una ontología y taxonomías para la evaluación de la resiliencia[13].

Una vez que se tiene la capacidad de tener una medida objetiva de la resiliencia es posible realizar la gestión de la misma a lo largo del tiempo. Para ello se han desarrollado modelos de gestión de la ciberresiliencia, como el CERT® Resilience Management Model (CERT-RMM) que presenta la universidad Carnegie-Mellon[14]. Este modelo de gestión de la ciber-resiliencia pretende dar una visión unificada y convergente de las disciplinas de gestión de la seguridad, continuidad de negocio y la gestión de las operaciones de información y comunicaciones y aplicar el concepto de proceso a dichas disciplinas para poner en práctica los principios de mejora continua utilizando las métricas expuestas en los párrafos anteriores. El modelo contiene veintiséis procesos que cubren cuatro áreas para la gestión de la resiliencia: gestión de negocio, ingeniería, operación y gestión de procesos.

Basado en el anterior, se han desarrollado modelos de autoevaluación, como el Cyber Resilience Review (CRR) desarrollado por el US-CERT[15] para determinar la resiliencia de la organización y la implantación de las prácticas de seguridad. Se basa en la idea de que toda

[10] Deb Bodeau, Rich Graubart, Len LaPadula, Peter Kertzner, Arnie Rosenthal, Jay Brennan Cyber Resiliency Metrics, ©2012The MITRE Corporation.
[11] Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report ENISA European Network and Information Security Agency (ENISA), 2010
[12] Measurement Frameworks and Metrics for Resilient Networks and Services: Challenges and Recommendations. ENISA European Network and Information Security Agency (ENISA), 2010
[13] Ontology and taxonomies of resilience, ENISA European Network and Information Security Agency 2011
[14] Richard A. Caralli, Julia H. Allen, Pamela D. Curtis, David W. White, Lisa R. Young CERT Resilience Management Model, Version 1.0 Software Engineering Institute, Carnegie Mellon 2010
[15] Cyber resilience review: self assesment package. US-CERT - Homeland Security 2014

organización despliega sus recursos (personal, información, tecnología e instalaciones) para dar soporte a misiones operativas específicas. Aplicando este principio, el CRR intenta comprender las capacidades de la organización para llevar a cabo, planificar, gestionar, medir y definir las prácticas de ciberseguridad en los siguientes dominios de gestión: recursos, control, configuración y cambio, vulnerabilidad, continuidad de servicio, riesgo, dependencia externa, preparación y concienciación y concienciación situacional.

También en España, y desde el INCIBE[16], se ha desarrollado un marco de medición de indicadores de ciber-resiliencia orientado a la ciberseguridad de las organizaciones, integrando los indicadores bajo la óptica de gobernanza, medidas de riesgo en los distintos dominios funcionales, e indicadores de rendimiento.

Finalmente, destacar cómo el desarrollo de ejercicios y modelos de simulación, como se establece en la Estrategia de Ciberseguridad Nacional, es una herramienta apropiada para la evaluación directa de la velocidad de respuesta de la dirección, la flexibilidad de la organización, la preparación del personal, los procedimientos, etc., sobre escenarios que recreen cualquier tipo de crisis.

CAMBIANDO A UNA VISIÓN A LARGO PLAZO

Gestionar una organización para alcanzar un elevado grado de ciber-resiliencia supone cambiar de las políticas de empresa orientadas a la maximización de beneficios a muy corto plazo por una planificación con objetivos a largo plazo. Como toda estrategia de seguridad sobre las que se construye la ciber-resiliencia, supone añadir costes adicionales a los procesos, inversiones cuyas ventajas no se harán evidentes en las cuentas de resultados del próximo ejercicio. Y eso es un cambio radical frente a la forma en la se concibe actualmente tanto la dirección económica como política de las organizaciones. La resiliencia supone la creación de organizaciones sostenibles, con estructuras adaptadas a conseguir metas a largo plazo, y la vuelta al compromiso real del personal y de la dirección con la organización.

La resiliencia será una cualidad total de la organización. No se puede trabajar para alcanzar únicamente la ciber-resiliencia como algo aislado, sino que implica acciones en todas las dimensiones de la organización. Para que los sistemas TIC tengan unos cimientos estables que permitan construir una infraestructura ciber-resiliente, los procesos de la empresa a los que dan soporte han de ser sostenibles, han de ser resilientes.

Ciber-resiliencia será el resultado de un largo proceso que implicará la capacidad de analizar críticamente el entorno, tener capacidad de anticipación, incorporar estructuras, actores y funciones flexibles y adaptables[17]. No es un estado, sino un conjunto de condiciones dinámicas que forma parte del espíritu de la organización. Por otro lado, la supuesta resiliencia no ha de ser una excusa para la relajación de la gestión del riesgo ni del cambio, ya que ambos procesos forman parte de los mecanismos para garantizarla.

[16] Suárez, Héctor, et al. Ciber-resiliencia Aproximación a un marco de medición. INTECO

[17] Norris, F.H., Stevens, S.P., Pfefferbaum, B., Wyche K.F., Pfefferbaum, R. L. (2008) 'Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness', *American Journal of Community Psychology* 41: 127–150.

A diferencia de otros principios de seguridad, la ciber-resiliencia no se implementa. La resiliencia forma parte del «ser» de la empresa: se es resiliente o no se es resiliente. Como se ha señalado a lo largo de este texto, la resiliencia, así como la ciber-resiliencia forman parte de la naturaleza de una organización. Por lo tanto, conseguir que una organización llegue a ser ciber-resiliente puede suponer cambiar dicha naturaleza y realizar una transformación profunda tanto en su estructura como en su forma operar. Esto no es algo para nada sencillo, esa transformación es en sí misma traumática y puede resultar en un cambio muy complejo. No se conseguirá con un manual de buenas prácticas, unos cursos de formación y un diploma. Es mucho más que eso. Supone sacrificar privilegios de algunos miembros de la organización, costumbres consagradas por el uso, la mentalidad de la dirección, los mandos intermedios y los trabajadores y las formas de trabajar. Supone renunciar a los caminos «fáciles», ser muy críticos con las modas y los cantos de sirena. La búsqueda de la resiliencia resultará incómoda para aquellos que se aferren a la consecución de objetivos a corto plazo.

Las bases económicas y sociales se han construido en un entorno en red sobre-conectado e interdependiente a nivel de personas, procesos y objetos. Es muy difícil que una organización sobreviva en un entorno que es no resiliente en sí mismo, sobre todo si se permite que en dicho entorno se generen fracturas sociales. Una empresa en un sector económico, o un estado, no resiliente tendría que adoptar estrategias muy radicales para asegurar su supervivencia, tal vez de tal calibre que mediatizasen su éxito a corto plazo. Garantizar un entorno estable y confiable ha de ser un esfuerzo conjunto que ha de implicar a entidades públicas y privadas.

Por lo tanto, alcanzar la auténtica ciber-resiliencia ha de ser un objetivo tanto del Estado como de las empresas, no se podrá conseguir la resiliencia de uno sin los otros. Esta meta se puede considerar una obligación cuando se está hablando de sectores de la administración pública, de compañías en sectores estratégicos o que tengan una importante dependencia en sus modelos de negocio de las tecnologías de la información y de las comunicaciones.

[i]

*Luis de Salvador Carrasco**
Doctor en Informática